# CHAIRMAN OF THE JOINT CHIEFS OF STAFF NOTICE

J-6 CJCSM 6510.01 CH 3
DISTRIBUTION: A, B, C, J, S 8 March 2006

CHANGE 3 TO CJCS MANUAL 6510.01

1. Page Substitution. Holders of CJCSM 6510.01, 25 March 2003, CH 2, 26 January 2006, "Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)" are requested to make the following page substitutions:

| Remove Page(s) | Add Page(s) |
|---|---|
| vii to xvi | vii to xvi |
| B-B-1 to B-B-22 | B-B-1 to B-B-6 |
| | B-B-A-1 to B-B-A-12 |
| | B-B-B-1 to B-B-B-20 |
| | B-B-C-1 to B-B-C-18 |
| | B-B-D-1 to B-B-D-2 |
| | B-B-E-1 to B-B-E-4 |
| D-1 to D-6 | D-1 to D-6 |
| GL-1 to GL-32 | GL-1 to GL-34 |

2. Summary of Changes. This change replaces the Table of Contents; Appendix B to Enclosure B, "Incident and Vulnerability Reporting;" Enclosure D, "References;" and updates the Glossary.

3. When the prescribed action has been taken, this transmittal should be filed behind the record of changes page in the basic document.

4. This manual is approved for public release; distribution is unlimited. DOD components (to include the combatant commands), other Federal agencies, and the public may obtain copies of this notice through the

Internet from the CJCS Directives Home Page--http://www.dtic.mil/cjcs_directives. Copies are also available through the Government Printing Office on the Joint Electronic Library CD-ROM.

For the Chairman of the Joint Chiefs of Staff:

Scott S. Custer

SCOTT S. CUSTER
Major General, USAF
Vice Director, Joint Staff

Enclosure(s):

Appendix B to Enclosure B – Incident Handling Program
Glossary

# LIST OF EFFECTIVE PAGES

The following is a list of effective pages. Use this list to verify the currency and completeness of the document. An “O” indicates a page in the original document.

| PAGE | CHANGE | PAGE | CHANGE |
|---|---|---|---|
| 1 thru 2 | O | C-F-1 thru C-F-2 | O |
| i thru xvi | 3 | C-G-1 thru C-G-2 | O |
| A-1 thru A-2 | O | C-G-A-1 thru C-G-A-4 | O |
| A-A-1 thru A-A-18 | O | C-G-B-1 thru C-G-B-4 | O |
| A-B-1 thru A-B-38 | O | C-G-C-1 thru C-G-C-2 | O |
| A-C-1 thru A-C-2 | O | C-G-D-1 thru C-G-D-6 | O |
| B-1 thru B-2 | O | C-H-1 thru C-H-10 | O |
| B-A-1 thru B-A-28 | 2 | C-I-1 thru C-I-8 | O |
| B-B-1 thru B-B-6 | 3 | C-I-A-1 thru C-I-A-6 | O |
| B-B-A-1 thru B-B-A-12 | 3 | C-I-B-1 thru C-I-B-4 | O |
| B-B-B-1 thru B-B-B-20 | 3 | C-J-1 thru C-J-14 | O |
| B-B-C-1 thru B-B-C-18 | 3 | C-K-1 thru C-K-6 | O |
| B-B-D-1 thru B-B-D-2 | 3 | C-K-A-1 thru C-K-A-6 | O |
| B-B-E-1 thru B-B-E-4 | 3 | C-L-1 thru C-L-2 | O |
| B-C-1 thru B-C-4 | O | C-M-1 thru C-M-2 | O |
| B-D-1 thru B-D-10 | O | C-N-1 thru C-N-8 | O |
| B-E-1 thru B-E-2 | O | C-I-A-1 thru C-I-A-6 | O |
| C-1 thru C-32 | O | C-O-1 thru C-O-8 | O |
| C-A-1 thru C-A-6 | O | C-P-1 thru C-P-2 | O |
| C-B-1 thru C-B-14 | O | D-1 thru D-6 | 3 |
| C-C-1 thru C-C-2 | O | GL-1 thru GL-34 | 3 |
| C-E-1 thru C-E-12 | O | | |

(INTENTIONALLY BLANK)

RECORD OF CHANGES

| Change No. | Date of Change | Date Entered | Name of Person Entering Change |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

Page

ENCLOSURE

Page

Page

FIGURE

TABLE

Page

# APPENDIX B TO ENCLOSURE B
# INCIDENT HANDLING PROGRAM

1. Purpose. This appendix provides joint guidance and methodology for incident handling on DOD systems. The program includes the responsibilities for specific organizations and individuals' roles for incident handling, which will be included in respective annexes in CJCSM 6510.01. Other subject areas include reporting procedures and handling procedures.

2. Background

a. Comprehensive reporting and response to reportable events and incidents is vital to ensuring commanders' successful accomplishment of their operational missions and continued operation of DOD's systems and networks.

b. Due to increased joint and combined operations, increased reliance on IT, increased threat to IT, and increased network centric operations requiring networks to be more resilient, the need for standardized incident handling practices across the Department of Defense is imperative.

c. Federal guidance mandates establishment of an incident response capability. The Federal Information Security Management Act (FISMA) of 2002 (reference lll) requires federal agencies to have in place incident detection and reporting mechanisms. Appendix III to Office of Management and Budget (OMB) Circular No. A-130 "Security of Federal Automated Information Resources" (reference qq), directs agencies to establish formal incident response mechanisms. DODI O-8530.01 (reference s) identifies five phases of CND: Protect, Monitor, Detect, Analyze, and Respond.

d. This appendix covers the DOD procedures pertaining to the last three phases. While robust protection will prevent many incidents, the dynamic nature of the CND environment requires vigilance in maintaining a unified DOD response plan. For this reason, CND components must maintain an effective CND monitoring capability to support incident and event detection.

e. Once suspicious activity is identified, a standard and unified response will greatly improve the Department of Defense's ability to react to incidents and maintain operations. Under ideal circumstances all of the below activities are performed. However, due to conflicting priorities, such as operational requirements and limited resources, organizations may not be able to perform all activities. Nevertheless, requirements specified for incident sets will not be disregarded due to the global threat to the Department of Defense. Under all circumstances components will provide incident and reportable event reports IAW this policy.

f. Term “system” used in this appendix refers to applications, enclaves, out-sourced IT-based processes and platform IT connections as defined in DOD Directive 8500.1 (reference bbb). An incident can impact a single system or multiple systems or a combination of information resources within a network or networks.

3. Basic Incident Handling Guidelines

a. A reportable event or incident should be reported IAW Annex B of this appendix. Events (including reportable events) and incidents should be detected, analyzed, and corrected at the level that is deemed most effective by the governing combatant command, Service, and/or agency (C/S/A) and field activity.

b. Incidents or sets of events (reportable events that may result in an incident) should be reported early. Once verified as an incident, reports and updates should be provided often and with enough granularity for all DOD analysts to determine corrective actions related to monitoring, detecting, analyzing, and responding to protect their DOD assets.

c. Incidents that may be classified in multiple categories are reported at the most severe category; e.g., a Category 1 root level intrusion incident that is caused by a less critical Category 5 Non-Compliance Activity event is reported as a Category 1 incident.

d. Deconfliction and coordination is done horizontally and vertically through law enforcement/counterintelligence (LE/CI), intelligence, technical, and management/oversight channels for assistance and situational awareness.

e. Commanders are ultimately responsible and accountable for their networks.

4. Incident Handling Terms

a. Incident. Assessed occurrence having actual or potentially adverse effects on an information system. (CNSS Instruction No.4009)

b. Incident Handling. The detection, analysis, and response to any event or incident for the purpose of mitigating any adverse operational or technical impact.

c. Event. Occurrence, not yet assessed, that may affect the performance of an information system. (CNSS Instruction No. 4009)

d. Incident Set. Any compilation of incidents and/or intrusion sets with similar characteristics.

5. Incident Handling Methodology

a. In the past, the Department of Defense used ad hoc and decentralized methodologies for incident handling. This approach resulted in a varied degree of timeliness of reporting and recovery from incidents. Many times commanders were not aware of their network's health because the network operator's procedures for incident handling did not require such reporting.

b. Responding to an incident is similar to other military operations. However, sometimes intelligence and technical information may come from sources unique to the CND environment, including sources outside the Department of Defense. Consequently, extensive coordination with the US Computer Emergency Response Team (US CERT), LE/CI organizations, the Intelligence Community (IC), and industry partners may be required. Timeliness in responding to incidents is essential to the success of any network-centric operation. The intention of this methodology is to help coordinate, deconflict, and execute an incident response in minutes or hours as opposed to days or weeks.

c. The methodology discusses the activities involved for a comprehensive incident handling process. The activities are logically organized, but during the lifecycle of an incident they may be done repetitively, in parallel, or sequentially, depending on the incident. Below is an outline of the incident handling methodology. For a more in-depth discussion on the steps in the incident handling methodology see Annex B.

(1) Detect. Detection of an event and/or incident may occur in various ways, such as through an automated detection system or an individual noticing that their system is not performing properly. Subsequently, an incident may be reported in various levels of detail and dependability. Below are some guidelines to follow for the detect phase of incident handling.

(a) Contain. Containment of the incident, event, or actions to mitigate the potential threat (e.g., taking the system offline, blocking the ports) will be taken by system administrators early in coordination with the supporting CND Service Provider (CNDSP) to protect the system or network to prevent any further contamination or intrusion. The supporting CNDSP will coordinate with LE/CI as required.

(b) Assess and Report. An event manifests in a variety of ways. Analysts assess if the event meets categorization outlined in Annex B as an event or incident. If it is a confirmed reportable event or incident, the reportable event or incident is categorized as outlined in Annex B and reported.

(c) Initiate documentation. Starting with the initial interview of the event observer, incident responders will document the potential incident and all actions taken during resolution of the incident. This is also the time to establish a chain of custody, as chain of custody is necessary for law enforcement purposes. (Note: It is better to establish a chain of custody and not use it than not to have a chain of custody and need one).

(d) Submit Initial Report. Report the occurrence of an event to the appropriate organizations and commands; see Incident Reporting Procedures in Annex C. Reporting of incidents and reportable events follow two channels in parallel -- technical and operational.

1. Operational Reporting. The operational reporting channel notifies commanders at all levels about the status of their systems or networks and the operational impact of the incident on mission(s). This channel is a vital conduit for the commanders to identify the operational impact and direct the incident handling process to mitigate any negative impact on their mission(s).

2. Technical Reporting. The technical channel mitigates the operational and technical impact of an incident on operation of the system or network.

3. Additionally, this is when the LE/CI community is notified of an incident and an investigation may be started IAW DOD Instruction 5505.3, “Initiation of Investigation By Military Criminal Investigative Organizations.”

4. The security classification of the incident is determined at this stage, IAW DODI O-3600.2 (reference u), or local C/S/A and field activity original classification authority (OCA) approved classification guidance. Incidents and reportable events will be reported at the appropriate classification level over the appropriate system, i.e., NIPRNET e-mail, or normal phone for unclassified incidents, SIPRNET or secure phone for SECRET incidents. Care should be taken to not use assets on the network that were potentially compromised to report the incident because the attacker may be monitoring the compromised network and

may be warned of its detection.

(2) Analyze

(a) Gather information. CNDSP incident handlers, depending upon the type of incident, collect all the information about the incident or reportable event, such as logs, personal accounts, etc. Additionally, gathering of all-source intelligence, technical information, and the current operational situation for consideration and evaluation may be required.

(b) Validate the incident. Review the gathered information for the type of intrusion method used and system shortcomings that caused the incident to occur. Determine if the incident is identified by USSTRATCOM or respective commands' Commander's Critical Information Requirements (CCIR) and report appropriately IAW Annex C of this document.

(c) Determine Impact. Analyze the information gathered to determine the organization and system operation impact caused by the incident IAW Annex C of this document.

(d) Coordinate with others. Conduct the initial coordination with parties that may be needed to assist with the incident or reportable event. Coordination cannot be overstressed and is a continuous process from the inception of the reportable incident through any post-response activities, to include prosecution of an offender. Coordination ensures that the identification and deconfliction of incident or reportable event response is vetted through all the parties that may be impacted by the response. Coordination is conducted vertically by submitting the initial incident report to alert higher headquarters and CND organizations that a potential reportable event or incident may be occurring or identified, as well as horizontally, between other networks that may be affected.

(e) Submit Follow-on Reports. Submit updated information on the incident and the progression of the response to make the higher CND organizations and/or headquarters aware of the situation IAW Annex C.

(f) Develop Courses of Action (COA).

1. Identify COAs to respond to the incident. The COAs include the actions necessary to respond to the reportable event or incident, fix the system and assess the risk for the system or network.

2. Under some instances, in coordination with CNDSP, the Commander may decide to leave the system vulnerable and accessible in

order to monitor the attackers activities. This may be to assist a LE/CI investigation or for network defense and operational purposes.

3. COAs may include CND Response Actions (CND RA), as outlined in USSTRATCOM CND RA concept of operations (CONOPS) ensuring COAs are in concordance with ASD (C3I) memorandum, 26 February 2003, "Guidance for Computer Network Defense Response Actions" (reference mmm). Analysis, comparison, and selection of the best COA should be done at the lowest command possible; e.g., the theater commander should be the approving authority for an incident response COA for their theater. USSTRATCOM, through Joint Task Force-Global Network Operations (JTF-GNO), reserves the right to re-direct all response actions for incidents that fall into a DOD Enterprise incident set.

(3) Respond. Eradicate the risk and take actions that remove the cause of the incident from the system or network. Improve the network defenses to include conducting a vulnerability assessment, if applicable. Actions that potentially impact traffic on the USSTRATCOM-protected IP list must be coordinated with JTF-GNO.

(a) Assist LE/CI. When appropriate, assist LE/CI personnel in investigating the incident.

(b) Recover From Incident. Fully restore data and systems with the necessary patches and fixes applicable to the incident. Conduct the necessary changes to network configuration, such as port blocking and updating anti-virus components. Compromised machine will need to be removed from the network, erased, and rebuilt from trusted media unless absolute system integrity is established.

(c) Submit Final Report. Submit the final report that closes out the incident. Ensure that all parties have completed the necessary actions for the response.

## ANNEX A TO APPENDIX B TO ENCLOSURE B

## RESPONSIBILITIES

1. Joint Staff, combatant commands, Services, Defense agencies, DOD field activities and joint activities will:

a. Comply with the DOD Incident Handling Program IAW DOD Instruction 8530.2 (reference g) and CJCSI 6510.01 (reference b).

b. Report reportable events and validate incidents through the technical and management channels IAW this appendix.

c. Report CND CCIR to higher headquarters that maintain situational awareness of CND CCIR.

d. Coordinate horizontally and vertically with all appropriate organizations (e.g., Tier 1, 2, 3, LE/CI, and IC) for incidents.

e. Document and report all incident-related information.

f. Comply with all directives (including but not limited to warning orders, operation orders, communication tasking orders, etc.).

g. Provide an inventory of the affected software, documents, etc., with an operational impact assessment of the potential data compromise to commanders, the IC community, LE/CI organizations, etc., to assist with investigations, as necessary.

h. Include requirements to comply with all portions of this program and stipulate its enforcement within all DOD IT/service contracts. C/S/A and field activity vendors, contractors, and suppliers must comply with the procedures contained within this document.

i. Coordinate with JTF-GNO on all incidents prior to coordinating or taking action outside of the Department of Defense, ensuring that the incident is not part of an incident set. If the incident is part of an incident set, prior approval by JTF-GNO is required before contacting any entity outside the Department of Defense. LE/CI organizations conducting lawfully assigned functions are not restricted from working with LE/CI counterparts outside of the Department of Defense. The LE/CI Center at JTF-GNO shall serve as the repository for relevant information shared by LE/CI community and providing a focal point for

LE/CI coordination with JTF-GNO.

j. Document support IA and CND operations with coalitions or allies.

2. Organizational Responsibilities

a. Global (Tier 1)

(1) United States Strategic Command (USSTRATCOM) will:

(a) Plan and execute operations to defend DOD computer networks or other vital national security interests, as directed by the Secretary of Defense, against any unauthorized computer network intrusions or attacks through the JTF-GNO.

(b) Issue incident or reportable event response orders and alerts through JTF-GNO to the C/S/As and field activities.

(c) Coordinate through the JTF-GNO with the IC Incident Response Center (IC-IRC), which operates under the authority of the IC chief information officer (CIO), on all matters relating to the governance, secure operations, and defense of the IC networks.

(d) Provide reports (summaries, significant incidents, trends, Enterprise-wide issues) to OSD through Joint Staff as required.

(2) JTF-GNO will:

(a) Ensure DOD C/S/As and field activities are informed on all Global NetOps issues.

(b) Assess operational impacts of possible COAs and weigh actions against the risk assessments to preserve the Global Information Grid (GIG).

(c) Direct and oversee procedures to provide department measures of effectiveness and battle damage assessment (BDA) during and following network defense operations.

(d) Serve as the central manager for all DOD Enterprise incident sets.

(e) Perform global incident/intrusion monitoring and detection, strategic vulnerability analysis, system forensics, media analysis, and responses to information assurance (IA)/CND-related activity.

(f) Direct COAs and coordinate IA and CND incident response actions across the Department of Defense to defend networks under attack.

(g) Determine COA and direct restoration of GIG capabilities and services when required.

(h) Coordinate CND support to the combatant commanders.

(i) Coordinate with and receive support from the LE/CI Center at JTF-GNO.

(j) Coordinate with the C/S/As and field activities in determining the technical and operational mission impacts caused by degradations, outages, and IA and CND events.

(k) Maintain situational awareness on all honeynets, honeypots, and other network deception systems to deconflict real or perceived GIG vulnerabilities and exploited GIG systems.

(l) Maintain “DOD Protected Traffic List” to ensure DOD critical systems maintain connectivity with the GIG.

(m) Coordinate with the Department of Homeland Security (DHS) for all incidents that involve the Department of Defense and other federal agencies. As appropriate, the JTF-GNO will notify and/or coordinate with the United States Computer Emergency Readiness Team (US-CERT) on incidents.

(n) Maintain and disseminate baseline DOD intrusion detection system (IDS) signature set.

(o) Coordinate with US CERT and Computer Emergency Response Team Coordination Center (CERT CC).

(p) Receive incident reports from CNDSP.

(q) Assess National Security Incident Response Center (NSIRC) products and coordinate results with impacted services and systems.

(r) Provide technical data to NSA to facilitate analysis.

b. Regional/Theater (Tier 2)

(1) Combatant command will:

(a) Monitor the combatant commander's GIG assets, determine operational impact of major degradations and outages, and coordinate responses to degradations and outages that affect joint operations to protect functional combatant command equities.

(b) Coordinate and report honeypots and other network deception systems to JTF-GNO, for situational awareness and correlation purposes, prior to connection to any DOD network.

(c) Leverage CND RA, as necessary, IAW ASD (C3I) memorandum, 26 February 2003, "Guidance for Computer Network Defense Response Actions" (reference mmm).

(d) Ensure system compliance with JTF-GNO orders and alerts and provide required updates to theater NetOps organizations.

(e) Exercise supporting command relationship to USSTRATCOM when incidents or actions have a global impact.

(f) Exercise supported command relationships with global NetOps organizations when incidents or actions have a theater impact.

(g) Establish MOA, in coordination with the DISA, with allied forces for the conduct of incident handling between the multinational forces.

(2) Service and Agency Global Network Operations and Security Centers (NOSCs)

(a) Coordinate problem resolution actions that affect global and theater operations.

(b) Implement JTF-GNO-directed policy and operational measures to ensure near real time, worldwide defense of the GIG.

(c) Establish procedures for dissemination of advisories, alerts, and warning notices, including those originating outside the Service and the Department of Defense.

(d) Report information to JTF-GNO for inclusion into the "DOD Protected Traffic List."

(e) Collect and consolidate service-wide reportable data.

(f) Coordinate and report honeypots and other network deception systems to JTF-GNO, for awareness and correlation purposes, prior to connection to any DOD network. In addition report, for situational awareness purposes, deployments within combatant command Service components to that combatant command.

(3) Non-intelligence community DOD agencies will:

(a) Coordinate, execute, and/or support troubleshooting and restoration actions for agency systems or networks.

(b) Implement policy and operational measures to ensure near real-time, worldwide defense for the agency's portion of the GIG NetOps.

(c) Establish procedures for dissemination of CND and related advisories, alerts, and warning notices.

(4) Global NetOps Support Center (GNSC)/Theater NetOps Centers (TNC) will:

(a) Issue technical and operational directives to Service Theater NOSCs/agency theater NOSCs to ensure compliance with Theater Network Control Center (TNCC) and/or JTF-GNO direction.

(b) Provide TNCC or Global Network Control Center (GNCC) with information security products and services IAW relevant MOA and service-level agreements (SLA), to include the monitoring and reporting of intrusions and analysis and correlation of intrusion incidents with components, sub-unified commands and joint task forces.

(c) Assist in determining the technical and operational mission impacts caused by degradations, outages, and IA and CND events.

(d) Perform theater incident and/or intrusion monitoring and detection, strategic vulnerability analysis, system forensics, media analysis, and responses to IA and CND-related activity for combatant command joint activities, including joint task forces, Joint Functional Component Commands (JFCC), and operating locations.

(e) Assist combatant commands in directing COAs and coordinating the IA and CND incident response actions across the theater to defend systems or networks under attack.

(f) Recommend COAs and coordinate restoral of capabilities and services when required.

(g) Identify and resolve computer security anomalies that affect the Theater Information Grid (TIG).

(h) Coordinate theater CND support as directed by the TNCC.

(i) Work with and receive support from LE/CI organizations.

(j) Support theater IA and CND operations with coalitions or allies.

(k) Provide assistance to LE/CI, as requested.

(5) Global Network Control Center (GNCC) will:

(a) Determine technical impact of major degradations and outages and coordinate technical responses.

(b) Execute or ensure compliance with the JTF-GNO directives with the support of the TNC and component NetOps forces.

(c) Establish operational priorities for and impact assessments of NetOps actions in support of their missions.

(6) Theater Network Control Center (TNCC) or Theater C4I Control Center (TCCC) will:

(a) Monitor the TIG and determine operational impact of major degradations and outages.

(b) Coordinate responses to TIG degradations and outages.

(c) Respond to JTF-GNO directions.

(d) Advise senior leadership and provide recommendations on COAs concerning NetOps issues having an operational impact on mission accomplishment.

(e) Direct, coordinate, and integrate response actions to computer network attacks and significant intrusions affecting the combatant commander's TIG.

(f) Direct the theater's compliance with JTF-GNO directives.

(g) Deconflict issues between the TNC and Service and/or agency NOSC.

(h) Assist the TNC and GNCC in tracking the status of NetOps events and determining the technical and operational mission impacts caused by NetOps events.

(i) Respond to a variety of threats using a range of response measures to preclude or detect and counter any threat.

(j) Establish operational impact assessments of NetOps actions in support of their missions.

(k) Provide analytical services to LE/CI, as required.

(7) DISA will:

(a) Provide Enterprise IA and CND services in support of USSTRATCOM.

(b) Provide IA and CND functions in support of Multinational Information Sharing (MNIS) Combined Enterprise Regional Information Exchange System (CENTRIXS) networks.

(c) Assist combatant commands with establishment of MOA with allied forces for the conduct of incident handling between the multinational forces.

(d) Report honeypots, honeynets, and other network deception projects to JTF-GNO and the combatant commands, for informational purposes, prior to connection to any DOD network.

(8) Sub-unified commands will:

(a) Establish, if necessary, C4 control centers and name them by region/country (e.g., C4 Control Center-Korea (CCC-K)).

(b) Serve as a single POC for supporting and supported elements for system and network services and reporting.

(c) Comply with GIG SA (visibility and status) reporting requirements for the portion of the TIG assigned to them by the combatant commander.

(d) Provide the TNCC with mission impact assessments of system and network events.

c. Operational/Tactical (Tier 3) Base/Post/Camp/Station (B/P/C/S) will: Comply with the NetOps direction from their global/theater NOSCs or TNCC/GNCC, as appropriate.

d. LE/CI Center at JTF-GNO will:

(1) Serve as the primary interface between the JTF-GNO and the Defense Criminal Investigative Organizations (DCIOs), DOD counterintelligence organizations, DHS Information Assurance Infrastructure Protection (IAIP), and other state and federal agencies for CND-related law enforcement and counterintelligence issues. Investigative agencies will keep the LE/CI Center informed of independently conducted coordination efforts that affects or impacts CND efforts.

(2) Receive operational direction through the Defense Cyber Operations Group (DCOG) from the DCIOs and respond to the information requirements of the Commander, USSTRATCOM (CDRUSSTRATCOM) and Commander, JTF-GNO.

(3) Coordinate, deconflict, and facilitate CND-related law enforcement and counterintelligence investigations and operations among the C/S/As and field activities.

(4) Provide analytical services to support CND investigations and operations.

(5) Support CND planning and policy development.

(6) Coordinate release of CND LE/CI information, with appropriate release authority, from originating agencies to support information sharing across the C/S/As and field activities.

(7) Deconflict operational orders/fragmentary orders that specifically address actions involving DOD Enterprise incident sets.

(8) Request operational assistance from LE/CI in support of operational orders/fragmentary orders.

e. NSA will:

(1) Provide tailored, all-source, current and long-term analysis addressing the threat(s) to the GIG.

(2) Provide analytical and operational support for CND RA IAW ASD(C3I) memorandum, 26 February 2003, "Guidance for Computer Network Defense Response Actions" (reference mmm).

f. Computer Network Defense Service Provider (CNDSP) will:

(1) Provide, in coordination with JTF-GNO, technical, analytical, and coordination services (e.g., the analysis and reporting of intrusions, incidents and events, dissemination of alerts and warning notices, computer diagnostics, short-term CND trend and pattern analysis, information assurance vulnerability management (IAVM) monitoring) to the DOD CNDSPs.

(2) Develop capabilities to track ongoing incident sets and determine if detected incidents match criteria for inclusion.

3. Individual Responsibilities

a. Designated approval authority (DAA) will:

(1) Ensure intrusion detection capabilities for installed systems.

(2) Ensure systems and subsystems potentially affected by CND incidents are isolated and, if necessary, are restored and/or rebuilt IAW this policy and relevant STIGs.

(3) Review incident reports and ensure corrective actions are taken to prevent future incidents.

(4) Ensure appropriate commanders are informed of all incidents.

b. Information assurance manager (IAM) will:

(1) Ensure incidents are properly reported to the DAA and the DOD reporting chain, as required, and that responses to IA-related alerts are coordinated.

(2) Ensure systems and subsystems potentially affected by CND incidents are isolated and, if necessary, are restored and/or rebuilt.

(3) Provide local organization policy and procedures for reporting and handling incidents.

c. Information assurance officer (IAO) will:

(1) In coordination with the IAM, initiate protective or corrective measures when an IA incident or vulnerability is discovered.

(2) Ensure systems and subsystems potentially affected by CND incidents are isolated and, if necessary, are restored and/or rebuilt.

d. System administrators/network administrators will:

(1) Immediately notify their operational chain and supporting CNDSP (e.g., network defense activity, NOSC) when incidents or intrusions are detected, and logically isolate the system to prohibit any additional malicious activities on the system, IAW mission requirements and DAA. Isolation includes physical isolation (unplugging the network connection), restricting any direct physical access, and logical isolation (blocking the IP at security routers or firewalls both inbound and outbound) from the network to the system.

(2) There will be instances where LE/CI requests that DOD system providers permit a potentially compromised DOD machine(s) to remain operational to facilitate law enforcement investigations or CI operations. This is further discussed in Annex C to this Appendix.

e. Users will: Report all security incidents immediately IAW local procedures and follow established reporting procedures for reporting criminal and/or security incidents.

f. Commanders will:

(1) Report events and incidents through command channels and notify local LE/CI.

(2) Provide OPREP 3 Pinnacle reports IAW CJCSM 3150.03B, “Joint Reporting Structure Event and Incident Reports” (reference nnn) through operational channels for incidents considered to have major mission impact (i.e., consider system MAC level). See Annex C, paragraph 3.

(INTENTIONALLY BLANK)

## ANNEX B TO APPENDIX B TO ENCLOSURE B

## INCIDENT HANDLING METHODOLOGY

1. Background

a. Incident response is similar to other military operations. However, it is important to note that in many instances, intelligence and technical information may come from sources unique to the CND environment, including sources outside the Department of Defense, and may require extensive coordination with US CERT, LE/CI organizations, IC, and industry partners. Timeliness is essential to the success of any network-centric operation. It is intended that the following methodology be utilized to coordinate, deconflict, and execute an incident response in minutes or hours as opposed to days or weeks.

b. The methodology discusses the activities involved for a complete incident handling process. **The activities are sequentially organized, but during the lifecycle of an incident they may be done repetitively, in parallel and sequentially, depending on the incident**.

2. Detect. Detection of an incident or reportable event may occur in various ways, such as through an automated system or an individual noticing that the system is not performing properly. Subsequently, an incident may be reported in various levels of detail and dependability. Below are guidelines to follow for the detect phase of incident handling.

a. Detect the incident or reportable event

(1) An event can manifest in a variety of ways. Below is a list of examples of events that may indicate an incident:

(a) The network intrusion detection sensor sends alerts for suspicious network traffic.

(b) The antivirus (AV) software alerts that a device is infected with a worm, virus, or other form of malicious logic.

(c) A Web server crashes.

(d) Users complain of slow access to hosts on the Internet or mail servers.

(e) The system administrator sees a filename with unusual characters.

(f) The user calls the help desk to report a threatening e-mail message.

(g) The system records a suspicious configuration change in its log.

(h) A system logs multiple failed login attempts from an unfamiliar remote system.

(i) The e-mail administrator sees a large number of e-mails with suspicious content.

(j) The network administrator notices deviation from typical network traffic flows.

(k) The firewall administrator may see outbound deviant connections not seen by other means.

(2) Next, analysts assess the event and determine if it is a reportable event or confirmed incident. If it is a reportable event or confirmed incident, it is categorized and the incident handling methodology is followed.

(3) Incident categorization is defined according to the framework outlined in Table B-B-B-1. In cases where more than one category applies, the most severe applicable category is chosen.

| Category | Description | Description Purpose |
|---|---|---|
| **1** | **Root Level Intrusion (Incident)**: Unauthorized privileged access (administrative or root access) to a DOD system. | – Modify<br>– Take<br>– Add<br>– Delete<br>– Unknown |
| **2** | **User Level Intrusion (Incident)**: Unauthorized non-privileged access (user-level permissions) to a DOD system. Automated tools, targeted exploits, or self-propagating malicious logic may also attain these privileges. | – Modify<br>– Take<br>– Add<br>– Delete<br>– Unknown |
| **3** | **Unsuccessful Activity Attempt (Event)**: Attempt to gain unauthorized access to the system, which is defeated by normal defensive mechanisms. Attempt fails to gain access to the system (i.e., attacker attempt valid or potentially valid username and password combinations) and the activity cannot be characterized as exploratory scanning. Can include reporting of quarantined malicious code. | |
| **4** | **Denial of Service (Incident)**: Activity that impairs, impedes, or halts normal functionality of a system or network. | – Denial of Service |
| **5** | **Non-Compliance Activity (Event)**: This category is used for activity that due to DOD actions (either configuration or usage) makes DOD systems potentially vulnerable (e.g., missing security patches, connections across security domains, installation of vulnerable applications, etc.). In all cases, this category is not used if an actual compromise has occurred. Information that fits this category is the result of non-compliant or improper configuration changes or handling by authorized users. | – Vulnerability |
| **6** | **Reconnaissance (Event)**: An activity (scan/probe) that seeks to identify a computer, an open port, an open service, or any combination for later exploit. This activity does not directly result in a compromise. | – Identify |
| **7** | **Malicious Logic (Incident)**: Installation of malicious software (e.g., Trojan, backdoor, virus, or worm). | – Modify<br>– Take<br>– Add<br>– Delete<br>– Unknown |

Table B-B-B-1. Incident and Reportable Event Categorization

| | | |
|---|---|---|
| **8** | **Investigating (Event)**: Events that are potentially malicious or anomalous activity deemed suspicious and warrants, or is undergoing, further review. No event will be closed out as a category 8. Category 8 will be recategorized to appropriate Category 1-7 or 9 prior to closure. | – Attempted Access<br>– Anomalous Activity<br>– Questionable Software |
| **9** | **Explained Anomaly (Event)**: Events that are initially suspected as being malicious but after investigation are determined not to fit the criteria for any of the other categories (e.g., system malfunction or false positive). | – System malfunction<br>– False report |

Table B-B-B-1. Incident and Reportable Event Categorization (cont.)

b. Initiate documentation. Begin documenting the potential incident and all actions taken for resolution of the incident. This is also the time to establish a chain of custody over any data, if it is necessary for law enforcement. (Note: It is better to establish a chain of custody and not use it than not to have a chain of custody and need one).

c. Contain incident or reportable event

(1) Contain the incident or reportable event by taking necessary mitigation actions against the potential threat and to protect the system or network from further exploitation (i.e., take the affected system offline or block any exploited ports). Perform containment early in order to protect the system or network and to prevent any further contamination.

(2) In some instances, after consultation with the servicing CNDSP, the commander may decide to leave the affected system's vulnerability accessible in order to monitor the attacker's activities. CNDSPs will monitor an attacker's activities at all times regardless of LE/CI involvement. This monitoring for system protection purposes is conducted in the ordinary course of business and authorized by federal law. The results of monitoring for network defense may be shared with LE/CI organizations (18 USC 2511(2)(a)(i)) (reference ooo). CNDSPs are not authorized to conduct monitoring on behalf of LE/CI organizations for purely LE/CI purposes unrelated to CND. LE/CI organizations must consult their servicing Staff Judge Advocate (SJA) regarding monitoring conducted pursuant to those independent LE/CI authorities.

d. Submit initial report. Report the occurrence of an incident or potential incident to the appropriate organizations and commands (see Incident Reporting Procedures in Annex C).

(1) Notification of incidents against DOD non-national security systems also requires coordination among Services, Defense agencies, and other Defense components. Timely notification of incidents supports CND by initiating the response process and warning dissemination to commanders, CND analysts, users, and information system administrators. The Reporting Timelines Table (Table B-B-B-2) is designed to expedite reporting of those incidents where national-level coordination and action may serve to mitigate or prevent damage to the GIG. Additionally, abbreviated reporting timelines extend the amount of time available for CNDSP to collect, process, and correlate information concerning reportable events and incidents before reporting them at the national level.

(2) Nothing in this manual shall preclude the rapid reporting of any event deemed necessary by the responsible CNDSP or CCIR. Certain Category 1, 2, 4, and 7 incidents are reportable using OPREP 3 reporting procedures and structure IAW CJCSM 3150.03B, "Joint Reporting Structure Event and Incident Reports" (reference nnn) (see Annex C or further information on Operational Reporting Structure (OPREP) 3 reporting requirements).

| Category | Severity | Initial Telephonic Report to Next Tier | Initial Report (e-mail or message) to next Tier | Minimum Reporting |
|---|---|---|---|---|
| 1<br>Root Level Intrusion[*]<br>(Incident) | Severe:<br>• Classified network<br>• Impacts current or planned operations<br>• Crosses C/S/A and field activity boundaries<br>• Involves a guard device<br>• Adverse impact on MAC I or MAC II system or network infrastructure (e.g. H-root, G-root, Generic Top Level Domain (GTLD) Domain Name Service (DNS) servers and backbone routers) | Immediately (standard within 15 min of discovery or awareness) (See Annex C for further guidance) | Within 4 hours of discovery or awareness | Tier 1<br>(JTF-GNO via CNDSP) |

Table B-B-B-2. Reporting Timelines

[*] May require OPREP 3 Reports IAW Annex C, para 2

| Category | Severity | Initial Telephonic Report to Next Tier | Initial Report (e-mail or message) to next Tier | Minimum Reporting |
|---|---|---|---|---|
| 1<br>Root Level Intrusion[*]<br>(Incident)<br>(Continued | Moderate<br>• Adverse impact on MAC III system or network infrastructure | As soon as practical (standard within 2 hours of discovery or awareness) | Within 8 hours of discovery or awareness | Tier 1<br>(JTF-GNO via CNDSP) |
| | Low:<br>• Not Applicable | N/A | N/A | N/A |
| 2<br>User Level Intrusion[*]<br>(Incident) | Severe:<br>• Classified network<br>• Impacts current or planned operations<br>• Involves a guard device<br>• MAC I/II system | Immediately (standard within 15 min of discovery or awareness) (See Annex C for further guidance) | Within 4 hours of discovery or awareness | Tier 1<br>(JTF-GNO via CNDSP) |
| | Moderate<br>• Involving Office of Secretary of Defense (OSD) network<br>• Adverse impact on DOD networks infrastructure (e.g. H-root, G-root, GTLD DNS servers and backbone routers) | As soon as practical (standard within 2 hours of discovery or awareness) | Within 8 hours of discovery or awareness | Tier 1<br>(JTF-GNO via CNDSP) |
| | Low:<br>• All other user-level intrusions | As soon as practical (standard within 2 hours of discovery or awareness) | Within 8 hours of discovery or awareness | Tier 1<br>(JTF-GNO via CNDSP)) |
| 3<br>Unsuccessful Activity Attempt<br>(Event) | All unsuccessful activity events | As soon as practical (standard within 4 hours of discovery or awareness) | Within 12 hours of discovery or awareness | Tier 2<br>(CNDSP with input into JCD within 24 hours of discovery) |

Table B-B-B-2. Reporting Timelines (cont.)

[*] May require OPREP 3 Reports IAW Annex C, para 2

| Category | Severity | Initial Telephonic Report to Next Tier | Initial Report (e-mail or message) to next Tier | Minimum Reporting |
|---|---|---|---|---|
| 4<br>Denial of Service[*]<br>(Incident) | Severe:<br>• Classified network<br>• Impacts current or planned operations<br>• Crosses C/S/A and field activity boundaries<br>• Involves a guard device<br>• Impacts operational mission of B/P/C/S level or higher networks<br>• MAC I/II system | Immediately (standard within 15 min of discovery or awareness) (See Annex C for further guidance) | Within 4 hours of discovery or awareness | Tier 1 (JTF-GNO via CNDSP) |
| | Moderate<br>• Crosses internal C/S/A and field activity enclave boundaries | Immediately (standard within 15 min of discovery or awareness) (See Annex C for further guidance) | Within 4 hours of discovery or awareness | Tier 1 (JTF-GNO via CNDSP) |
| | Low<br>• MAC III system | As directed by C/S/A and Field Activity Guidance | As directed by C/S/A and Field Activity Guidance | Tier 1 (JTF-GNO via CNDSP) |
| 5<br>Non-Compliance Activity (Event) | All Non-Compliance Events | As soon as practical (standard within 4 hours of discovery or awareness). | Within 12 hours of discovery or awareness. | Tier 2 (CNDSP) |

Table B-B-B-2. Reporting Timelines (cont.)

[*] May require OPREP 3 Reports IAW Annex C, para 2

| Category | Severity | Initial Telephonic Report to Next Tier | Initial Report (e-mail or message) to Next Tier | Minimum Reporting |
|---|---|---|---|---|
| 6<br>Reconnaissance<br>(Event) | Severe:<br>• Unauthorized scans between DOD controlled system(s) over DOD classified networks | Immediately (standard within 15 min of discovery or awareness) | Within 12 hours of discovery or awareness | Tier 1 (JTF-GNO via CNDSP) |
| | Moderate:<br>• Unauthorized scans between DOD controlled systems on DOD unclassified networks.<br>• Significant reconnaissance activity that can provide actionable information to the IA communities and IC.<br>(Note: These reports are used for trending analysis.) | As soon as practical (standard within 24 hours of discovery or awareness) | Within 72 hours of discovery or awareness | Tier 2 (CNDSP with input into JCD within 24 hours of discovery) |
| | Low:<br>• All other reconnaissance events | As directed by C/S/A and field activity guidance | As directed by C/S/A and field activity guidance | Tier 2 (CNDSP with input into JCD within 24 hours of discovery) |

Table B-B-B-2. Reporting Timelines (cont.)

| Category | Severity | Initial Telephonic Report to Next Tier | Initial Report (e-mail or message) to Next Tier | Minimum Reporting |
|---|---|---|---|---|
| 7<br>Malicious Logic[*]<br>(Incident) | Severe:<br>• Infection by a previously unknown virus, 0-day exploit, or viruses that directly affect global network services<br>• Detection of any new or unknown unauthorized/ hidden processes or hidden kernel modules<br>• Discovery of new virus whose propagation could potentially outrun DOD containment<br>• MAC I/II system | Immediately (standard within 15 min of discovery or awareness) (See Annex C for further guidance) | Within 4 hours of discovery or awareness | Tier 1 (JTF-GNO via CNDSP) |
| | Moderate:<br>• Distributed network attack tool or daemon<br>• Unauthorized remote network tools, Trojans, or other stealthy backdoor tools present | As soon as practical (standard within 2 hours of discovery or awareness) | Within 8 hours of discovery or awareness | Tier 2 (CNDSP with input into JCD within 24 hours of discovery) |
| 8<br>Investigating<br>(Event) | Not applicable | Acknowledgment from asset owner as soon as practical, (standard within 2 hours of notification) | Consistent with the most severe possible interpretation (see above) | Tier 2 (CNDSP with input into JCD within 24 hours of discovery) |
| 9<br>Explained Activity (Event) | Not applicable | None | As soon as practical | Tier 1 (JTF-GNO via CNDSP) |

Table B-B-B-2. Reporting Timelines (cont.)

Note: These requirements do not supersede those requirements established by USSTRATCOM CND CCIRs. These CCIRs may be found on JTF-GNO's Web site at http://www.jtfgno.smil.mil/index.cfm?Page=CCIR-PIR.

[*] May require OPREP 3 Reports IAW Annex C, para 2

e. Incident and reportable event reporting follows two channels in parallel: technical and management/oversight. The technical channel is designed to assist with the handling of incidents and provide fixes to mitigate the operational and/or technical impact of an incident. The management and oversight channel is designed to notify commanders at all levels of the ability of their systems to support operations and the operational impact of the incident; this is when the LE/CI community is notified of an incident and an investigation may be started. The management and oversight channel is also a conduit for the commander to guide the incident handling process to mitigate any additional negative impact on their information systems.

f. Additionally, security classification of the incident is determined at this stage, IAW DODI O-3600.2 (reference u). Incident reports will be protected based on their classification and sensitivity. All incidents occurring on the SIPRNET shall be classified at least SECRET. Classifying an incident higher than SECRET will depend upon the classification level of the material involved (e.g., TOP SECRET or compartmented), overall impact, and compromise potential. Incidents occurring on NIPRNET systems will be unclassified and marked FOUO unless an adversary's exploitation of information in the report would result in classified information compromise or present a significant negative impact on a national security organizational mission.

g. Reports should be submitted based upon the most protected means available for the affected system. Use SIPRNET or secure phone/fax if those systems are available. The use of unclassified reporting means (NIPRNET, nonsecure fax) should only be used for incidents on unclassified systems. JTF-GNO will work with NOSCs, TNCs, and GNCCs/TNCCs to correlate and deconflict incident reporting information. Potentially compromised assets will be removed from the network prior to reporting an incident to remove the threat of an attacker monitoring the compromised network and potentially intercepting the incident report (see Annex C for further guidance on submitting reports). Table B-B-B-3 summarizes reporting vehicles in use in their order of preference for reporting.

| Order | Method | Use |
|---|---|---|
| DATA | | |
| 1 | JCD SIPRNET | All levels |
| 2 | Defense Message System (DMS) SIPRNET (Record message traffic) | All levels |
| 3 | E-mail SIPRNET | All levels |
| 4 | DMS NIPRNET | All levels |
| 5 | NIPRNET with security protection (e.g., encryption) | All levels |
| 6 | NIPRNET, with no security protection (e.g., encryption) | All levels |
| Fax/Voice | | |
| 1 | Secure Fax | All levels |
| 2 | Secure Telephone Unit (STU)-III/Secure Telephone Equipment (STE) | All levels |
| 3 | Defense Red Switch Network (DRSN) | All levels |
| 4 | Nonsecure Fax | All levels |
| 5 | Defense Switched Network (DSN) | All levels |

Table B-B-B-3. Reporting Vehicles

3. Analyze

a. Gather information. Collect all the information about the incident, such as logs, personal accounts, inventory of the systems, etc. Additionally, gathering all-source intelligence, technical information, and the current operational situation for consideration and evaluation may be required.

b. Validate the incident or reportable event.

(1) Review the gathered information for the type, intrusion method used, and system shortcomings of the incident.

(2) Determine if the incident is a USSTRATCOM or other commands' CCIR and report appropriately. The USSTRATCOM's CCIR are a set of specific operational reporting criteria that enumerate unauthorized results, deemed by JTF-GNO to be the best indicators of an incident having strategic significance. They are intended to refine reporting requirements. The JTF-GNO is responsible for maintaining and updating USSTRATCOM's CCIR list and publishing updates in the form of a message. CCIR messages will be serialized to ensure continuity and may be maintained on the SIPRNET on the JTF-GNO SIPR Web page. Incidentally, any reporting unit may, through normal reporting channels, recommend CCIR updates. Component commanders may add to this list for reporting unique items of interest.

(3) Verify the incident is categorized properly, per Table B-B-1.

(4) Determine the attack vector used by the threat actor. The attack vector is defined as the primary method the threat actor used to cause the incident or reportable event. In this category, the system owner does not have any influence on the type of activity that occurs against the DOD system. Table B-B-B-4 is the list of the attack vectors.

| Attack Vector Category Number | Description |
|---|---|
| 1 | Exploited New Vulnerability: This vulnerability was unknown prior to the event or there was no mechanism available to prevent it. |
| 2 | Exploited Known Vulnerability: This vulnerability was known prior to the event and there was a mechanism available to prevent it. |
| 3 | Self-Propagating Malicious Logic: A script which upon release requires no further intervention by persons or groups to achieve malicious effect on a system or network. |
| 4 | Insider Purposeful: A user knowingly took specific actions that jeopardized DOD systems or data. |
| 5 | Insider Accidental: A user took actions that had consequences over and above the intentions and jeopardized DOD systems or data. |
| 6 | Distributed Network Activity: Activity from multiple IP addresses, which overwhelms system or network resources. |
| 7 | Non-Distributed Network Activity: Activity from a single IP address that overwhelms system or network resources. |
| 8 | Network Scan: Activity that targets multiple IP addresses. This is referred to as a horizontal scan. |
| 9 | System Scan: Activity that targets a single IP address across a range of ports. This is referred to as a vertical scan. |
| 10 | Other System Compromise: Compromise resulting from access previously gained on another DOD system. The description should include whether the other system was in the same B/P/C/S enclave, in the same DOD enclave (C/S/A and field activity), or in a different DOD enclave. |
| 11 | Reconnaissance: Coordinated probing, scanning, or other activity that is used to identify DOD systems for exploitation. |
| 12 | Unknown: The intrusion is not covered by the listed methods. |

Table B-B-B-4. Attack Vector

(5) Determine the system weaknesses, which are the system configurations that should have been in place to prevent the incident from happening. Table B-B-B-5 provides causes of system compromises, areas that the Department of Defense can focus its efforts on the current response, and ways to prevent future intrusions. More than one weakness category may apply.

| Weakness Category Number | | Description |
|---|---|---|
| 1 | Sub-Category Number | AV Issue:  The incident could have been prevented if the system owner or administrator had implemented, configured, or updated the AV tools.  Further subcategories allow for the following options: |
| | A | No AV Signature:  In some instances, even though the administrators took all of the proper precautions, this is a new piece of malicious code that affects DOD systems and at the time was not detected by the companies providing AV signatures. |
| | B | AV Not Installed:  The infected system did not have any AV tool installed on it making it vulnerable.  If the AV tool had been installed, the system would have detected the malicious code and prevented it from making changes to the system. |
| | C | AV Not Turned On:  The system owner or administrator disabled the AV tool.  If the AV tool had been turned on, then the system would have detected the malicious code and prevented it from making changes to the system. |
| | D | AV Not Up-To-Date:  The system owner or administrator did not have the latest AV signatures installed, leaving the system vulnerable to known exploits. |
| | E | AV Not Properly Configured:  The system owner or administrator did not have the AV tool configured to detect all forms of malicious code (i.e., the AV tool did not scan all files on the hard drive or did not scan files prior to opening them). |
| 2 | Sub-Category Number | Patch Issue:  The incident was the result of a system owner or administrator not applying all of the appropriate patches to a particular system. |
| | A | Not Patched and No Information Assurance Vulnerability Alert (IAVA) Available:  The vulnerability did not meet the standards/criteria for issuing an IAVA, so while there is a patch available the system owner did not apply the patch. |
| | B | Not Patched But Within the IAVA Compliance Window:  The system was exploited using a vulnerability for which there is an IAVA but the compliance date for that particular IAVA is after the date of the compromise. |
| | C | Not Patched and IAVA Available, and Past the IAVA Compliance Window:  There is an existing IAVA that addresses the vulnerability but the system was not patched in accordance when it was compromised. |
| | D | Not Patched But Currently Under Extension:  There is an existing IAVA that addresses the vulnerability,but the system is under approved plan of action and milestones (POA&M) with mitigation to the IAVA compliance date due to programmatic considerations. |

Table B-B-B-5.  System Weakness

| Weakness Category Number Description | | Weakness Category Number |
|---|---|---|
| 2<br>(cont.) | Sub-Category Number | Patch Issue: The incident was the result of a system owner or administrator not applying all of the appropriate patches to a particular system. |
| | E | No Patch Available: This system was compromised because while the vulnerability exists, the vendor has not issued a fix to prevent the vulnerability from being exploited. |
| | F | Patch Installed But Not Effective: This system was patched yet the system was still compromised because the patch did not fix the problem. |
| 3 | Sub-Category Number | Configuration Issue: The incident is caused by a system setting (intentional or accidental) that allows an intruder to gain other than designated access to the system. |
| | A | Weak Passwords - A user name and password for system access or application access is easily guessed or blank. This does not apply to a system administrator installed application default password. |
| | B | Poor System Configuration: The system is configured so that it allows unauthorized or authorized users to gain additional access through applications or operating system settings. Examples of methods for gaining this type of access are targeting default settings, default installations of applications/operating systems, or default passwords. |
| | C | Poor Configuration Management: The system or network is configured in such a way that an intruder can use the system or network to conduct attacks against other systems, such as DOS; the system or network is not implemented in such a way as to separate its core assets from its publicly available assets; or the system or network is not designed with protection mechanisms in place, such as firewalls or IDS. |
| 4 | Sub-Category Number | Human Factors: An authorized or unauthorized individual violating DOD policy to compromise DOD systems and information by non-technical means. |
| | A | Social Engineering: Access was attempted or gained by an outsider gathering information on an individual or organization through non-technical means. |
| | B | Insider: An individual with authorized access to DOD systems or information took actions to purposefully or inadvertently circumvent security measures or to abuse their privileges. |
| | C | No Policy Available: An appropriate security policy or guidance is not in place. |
| | D | Policy Enforcement: The activity could have been prevented if proper training and enforcement of current policies had been implemented. |

Table B-B-B-5: System Weakness (cont.)

| Weakness Category Number Description | | Weakness Category Number |
|---|---|---|
| 5 | Sub-Category Number | Technical Means |
| | A | Compromised Information: The incident occurred because an individual or group had gained an insight into DOD information through technical means, such as sniffing packets on the wire, intercept, protected information being posted to a publicly available Web page, or other means. |
| | B | Network Trusted Exploitation: The incident was the result of interactions between DOD systems and exploitation of one system led to the compromise of another system. |
| | C | Unknown: The shortcoming is not covered by the above reasons. |
| 6 | Not Applicable | Other |

Table B-B-B-5: System Weakness (cont.)

c. Determine Impact. Analyze the information gathered and systems affected to determine the operational and technical impact of the incident.

(1) Operational Impact (OI). OI refers to detrimental effects to an organization's ability to perform its mission. This may include direct and/or indirect impacts that diminish or incapacitate system or network capabilities, the compromise and/or loss of mission critical data or the temporary or permanent loss of mission critical applications or systems. Examples of direct impact include: a secretary is unable to process temporary duty (TDY) orders, thus delaying personnel from performing TDY; an organization is unable to perform effective C2 with its parent/subordinate organization due to a disabled mail server; an organization cancels a tactical mission due to compromised mission plans or orders. Examples of indirect impact for a supply organization include: an Army division is unable to order/track/process repair parts using a networked system and is therefore unable to conduct combat operations due to insufficient availability of repair parts; barges on the Mississippi River are unable to deliver supplies caused by the inability of its crew to access the Department of Defense supplied river hazard data. Additionally, OI will include any detrimental impacts to time-phased force deployment data (TPFDD) based on direct or indirect incidents. For example, a Reserve unit goes unpaid, and as a consequence, the unit does not meet its deployment timelines.

(2) Technical Impact (TI). TI refers to the incident's detrimental impact to the technical capabilities of the organization. Assess the risk or threat level of a confirmed incident (Annex C has an incident criticality methodology that can assist with TI). TI typically refers to impacts on the network or system machines that are directly or indirectly affected by the incident. The TI may include network health status, potential data compromise or loss, equipment downtime or destruction, impact on other systems, or components (e.g., a machine removed from operations takes eight hours to be rebuilt; organizational commander authorized base unclassified LAN be disconnected from the NIPRNET until all infected machines were cleaned; a mail server was removed from the network and users were unable to access mail for six hours).

(3) When reporting TIs and OIs, the TIs are normally reported by the communications and technical component of an organization (J, G, S, N – 6), while OIs are typically reported by/to the operational component of an organization (J, G, S, N – 3). Examples: J-6 reports that an attacker accessed 3 MB of data from a server. J-3 reports attacker accessed 3 MB of unclassified family support group data and determines no operational impact.

d. Coordinate with others. Conduct the initial coordination with parties that may be needed to assist with the incident. Coordination cannot be overstressed and is a continuous process from the detection of the incident through any post-response activities, to include prosecution of an offender. Coordination ensures the identification and deconfliction of incident response COAs are vetted through all parties potentially impacted by the response. Coordination is conducted vertically by submitting the initial incident report to alert higher headquarters/CND organizations that a potential incident may be occurring or identified, as well as horizontally, between other networks that may be affected.

(1) Timely interagency coordination and deconfliction of operations is crucial to conducting an effective incident response. All Tier 1 incidents must be coordinated/deconflicted with the USSTRATCOM/JTF-GNO. Since the establishment of JTF-GNO, coordination/deconfliction of incidents with DISA is no longer required unless DISA is directly affected by the incidents.

(2) The process below includes procedures for coordinating and deconflicting both time-sensitive and non-time-sensitive operations. Time-sensitive operations generally involve network-centric COAs to defend the DOD GIG against imminent or ongoing threats. Non-time-sensitive operations include both network-centric and non-network-

centric COAs to defeat or mitigate ongoing threats such as a persistent, sophisticated intruder. While coordination and deconfliction are important and all inputs shall be considered by CDRUSSTRATCOM when deciding to approve or disapprove a particular course of action, non-concurrence from an organization does not constitute a veto over the operation.

(3) For the purposes of this policy, coordination and deconfliction are defined below:

(a) Coordination is the act of exchanging information between organizations to provide situational awareness, collaboration on assessments, and synchronized response actions.

(b) Deconfliction is a subset of coordination where information is shared to eliminate overlap or interference between ongoing activities.

(4) Time-sensitive operations require coordination inputs from the Department of Defense and non-DOD organizations with the timeliness required based on the threat and the operational situation as determined in the CCIR. As a general rule, inputs for time-sensitive operations will be required from all organizations within 4 hours of notification by USSTRATCOM or JTF-GNO. JTF-GNO J-2 will manage requests for IC coordination and deconfliction with the appropriate IC members. The LE/CI Center at JTF-GNO shall conduct LE/CI coordination and deconfliction with appropriate LE/CI organizations. Organizations participating in the coordination/deconfliction process shall provide POCs capable of responding 24 hours a day to take appropriate action or be able to recall necessary personnel who can complete the actions required within the required timeline IAW this manual.

(5) Non-time-sensitive coordination and deconfliction will use a more deliberative process employing periodic coordination/deconfliction meetings, correspondence, teleconferences and video teleconferences. Non-time-sensitive coordination and deconfliction procedures shall be used when JTF-GNO and USSTRATCOM contemplate non-network-centric COAs, such as diplomatic initiatives, public affairs campaigns, law enforcement informational exchanges with foreign countries, etc., or when network-centric Tier 1 incident responses are necessary but not assessed as time sensitive. Coordination/deconfliction meetings will be held periodically (e.g., weekly, bi-weekly) with the IC, appropriate DOD LE/CI organizations, the LE/CI Center, service components, JTF-GNO staff, and other government CND organizations as required.

(6) For Tier 1 level incident responses, the JTF-GNO will establish the coordination/deconfliction meeting frequency and ensure meeting notification is provided to appropriate organizations. For Tier 2 level responses, the respective C/S/A and field activity will establish the coordination/deconfliction meeting frequency and ensure meeting notification is provided to appropriate organizations, keeping JTF-GNO informed of any planned and executed incident responses.

(7) Initial notification and request for coordination and deconfliction shall include the following information at a minimum:

(a) A summary of the CND event to include: threat assessments, damage assessments, technical and operational impacts, and actions taken so far.

(b) Attribution assessment with levels of confidence.

(c) COAs under consideration and assessment.

(d) Time when inputs must be provided back to the incident response lead agency.

(8) Coordination/deconfliction inputs from the IC or LE/CI organizations for both time-sensitive and non-time-sensitive operations shall include a statement of understanding, where they may concur or nonconcur with proposed COAs. In cases where an organization nonconcurs, the organization shall provide supporting technical, operational, or policy information as required so the operational impact of COAs on those organizations can be balanced against the ongoing threat. Nonconcurrence does not equate to a veto.

(9) Organizations may recommend alternate COAs in cases where that organization nonconcurs with proposed COA. Organizations may provide assessments of the threat, potential collateral damage, operational impact, and political impact assessment for each COA and also recommend no action be taken for DOD, allied, and other forces networks. Organizations should also identify data discrepancies and corrected data if their organizations do not concur in that data provided by the incident response lead agency.

e. Submit Follow-on Reports. Submit updated information on the incident and the progression of the response to make the higher CND organizations and/or headquarters aware of the situation. Follow-on reports are submitted as directed by the higher CND organizations and/or headquarters. If no direction is provided, follow-on reports are submitted within 8 hours of new information being developed about the incident.

f. Develop COAs. Identify COAs to respond to the incident. The COAs include the actions necessary to respond to the incident, fix the system, return the system to operations, and assess the risk for the system or network. COAs may include CND RA in accordance with ASD (C3I) memorandum, 26 February 2003, "Guidance for Computer Network Defense Response Actions" (reference mmm). Analysis, comparison, and selection of the best COA from the ones developed should be done at the lowest command possible, e.g., the theater commander should be the approving authority for an incident response COA for the theater. USSTRATCOM, through JTF-GNO, reserves the right to oppose all response actions for incidents that fall into a DOD enterprise incident set or when actions otherwise affect multiple theater or Service networks.

4. Respond. Eradicate the risk and take actions that remove the cause of the incident from the system or network. All systems that have a Category 1 incident must be erased and rebuilt from trusted media, then patched and updated prior to connecting the system to the network to prevent an incident from recurring. Mission impact may require that the affected vulnerable component be mitigated temporarily until the mission allows the system to be rebuilt. For other categories, C/S/As and field activities have the discretion of rebuilding the system depending on the impact of the incident.

a. Assist LE/CI. Help LE/CI personnel investigate the incident and prosecute the perpetrators, if warranted. For more information on assisting LE/CI, see Annex C.

b. Recover from incident. Data and systems are fully restored with the necessary patches and fixes applicable to the incident. Conduct the necessary changes to network configuration, such as blocking ports and updating anti-virus signatures.

c. Submit final report and determine BDA.

(1) Submit the final report that closes out the incident. Incidents cannot be closed as a Category 8 (Investigating).

(2) Ensure all parties have completed the necessary actions for the response. BDA consists of the technical and operational impact the incident had on the organization and possible future operations security

(OPSEC) issues that may stem from the incident.

(3) Final Report and BDA is submitted 24 hours after the incident is resolved.

# ANNEX C TO APPENDIX B TO ENCLOSURE B

## REPORTING

1. Operational Practices

a. Technical Reporting Structure. The incident reporting community is organized into multiple tiers: Global (Tier 1), Regional/Theater (Tier 2), and Local (Tier 3). All incidents and reportable events are reported to the JTF-GNO.

(1) Local Level (Tier 3). Network service centers (NSCs) are at Service component headquarters, major commands, and Service elements at B/P/C/S or joint activities that serve as a focal point for reporting and handling incidents and network management at the lowest level.

(a) Service elements at B/P/C/S report, through Service-defined channels, to the Service or agency NOSC, or their CNDSP, which report to the JTF-GNO (see Figure B-B-C-1).

(b) Service elements subordinate to a commander of a combatant command simultaneously provides information reporting to a combatant command GNCC and TNCC, as directed by combatant command instruction or policy (see Figure B-B-C-1).

(c) Joint activities report incidents to their host command NSC, combatant command, and TNC (see Figure B-B-C-2).

(2) Regional/Theater (Tier 2)

(a) The TNCs provide direct support to the regional combatant commands, with CND services and technical reporting. TNCs are a component of the JTF-GNO (see Figure B-B-C-2).

(b) Service or agency NOSC.

1. Some Service NOSC architectures also include organizational elements that support regional components for the respective combatant commands or major commands. These organizations will vary from combatant command to combatant command.

2. Each Service and Defense agency NOSC providing CND services to a Service or Defense agency component supporting a regional combatant command make available warnings, reports, information, data, and statistics pertinent to the protection of resources assigned to the regional combatant command.

3. Service and Defense agency elements subordinate to a commander of a combatant command simultaneously report to a combatant command NetOps organization in addition to reporting to their Service or Defense agency NOSC or TNC. (See Figure B-B-C-1 and B-B-C-3). Reporting should be accomplished IAW combatant command guidance.

(2) Global (Tier 1). Tier 1 includes USSTRATCOM and JTF-GNO.

2. Intelligence Community

a. All C/S/As and field activities report incidents (or reportable events) affecting TS/sensitive compartmented information (SCI) networks directly to organizations as directed under SCI directives and policies as provided by the principal accrediting authority (PAA).

(1) All DOD SCI organizations (except NSA, National Reconnaissance Office (NRO), and National Geospatial-Intelligence Agency (NGA)) shall provide reporting directly to the DIA Information Assurance Protection Center (IAPC).

(2) Member organizations operating under authority of NSA, NRO, and NGA shall provide reporting to their agency authority IAW internal agency policy.

(3) All DOD IC members shall provide reporting of all reportable events directly to the IC-IRC within established reporting timelines.

b. All LE/CI matters and investigations regarding SCI networks, systems, and personnel shall be forwarded to the cognizant SCI LE/CI authorities, as responsibility is defined above.

c. The IC-IRC will ensure all TS/SCI reports are shared with JTF-GNO to ensure new vulnerabilities/exploits/incidents reported on compartmented systems are disseminated to the appropriate IC member organization for remediation.

d. All requests for DOD SCI information shall be vetted through the IC-IRC to the responsible community member organization.

3. <u>OPREP</u>

a. The following incidents are reportable using OPREP 3 reporting procedures and structure. For reportable event and incident category definitions and reporting timelines see Annex B. OPREP reporting procedures can be found in CJCSM 3150.03B (reference nnn).

(1) <u>Root Level Intrusion (Category 1)</u>. Intrusions (unauthorized control of a system and/or network by a personal computer or unauthorized computer) of MAC I or MAC II DOD information system(s).

(2) <u>User Level Intrusion (Category 2)</u>. User level (unauthorized user level permissions on a system) of MAC I or MAC II DOD information system(s).

(3) <u>Denial of Service (Category 4)</u>. DOS against MAC I or MAC II DOD information system.

(4) <u>Malicious Logic (Category 7)</u>. **Outbreak** (hostile code infecting DOD information system) **new malicious code** impacting operation and/or security of DOD information system. OPREP for previously reported outbreaks are not submitted (e.g., outbreak of virus reported two months ago).

b. The operational reporting structure is graphically shown in Figures B-B-C-1 through B-B-C-3.

c. JTF-GNO submits OPREP-3 for DOD-wide computer network incidents to USSTRATCOM.

4. <u>LE/CI Structure</u>. Information on computer anomalies and system or network incidents should be preserved to enable possible criminal prosecution or LE/CI operations.

a. Incidents should be reported to the appropriate LE/CI organization at the lowest level at which it is discovered IAW established C/S/A and field activity procedures.

b. The organization commander and/or director has the responsibility to engage LE/CI at JTF-GNO concerning a computer incident.

c. At a minimum, Category 1, 2, 4, and 7 incidents are reported to DOD LE/CI. All incidents involving potential or actual compromise of classified systems or networks are reported through standard CND technical reporting channels. Commanders may request investigations and LE/CI organizations determine if investigations are to be opened IAW DOD Instruction 5505.3, "Initiation of Investigation by Military Criminal Investigative Organizations."

d. The investigative community has substantial authority to access official government information and information from the private sector, consistent with normal investigative procedures. Ideally, the operational community should interface with the servicing LE/CI organization, which will in turn coordinate with LE/CI Center at JTF-GNO. The LE/CI Center disseminates information to other LE/CI organizations, including non-DOD LE/CI organizations, if appropriate.

e. Reporting incidents through LE/CI channels does NOT eliminate the requirement to report incidents through standard CND reporting channels.

5. Analysis and Correlation of Event and Incident Data. Analysis and correlation of event and incident data occurs at all levels, as well as within various functional communities (e.g., intelligence, counterintelligence, law enforcement, and communications).

6. Incident Reporting Diagrams. Figure B-B-C-1 through Figure B-B-C-3 present graphic representations of the incident report flow.

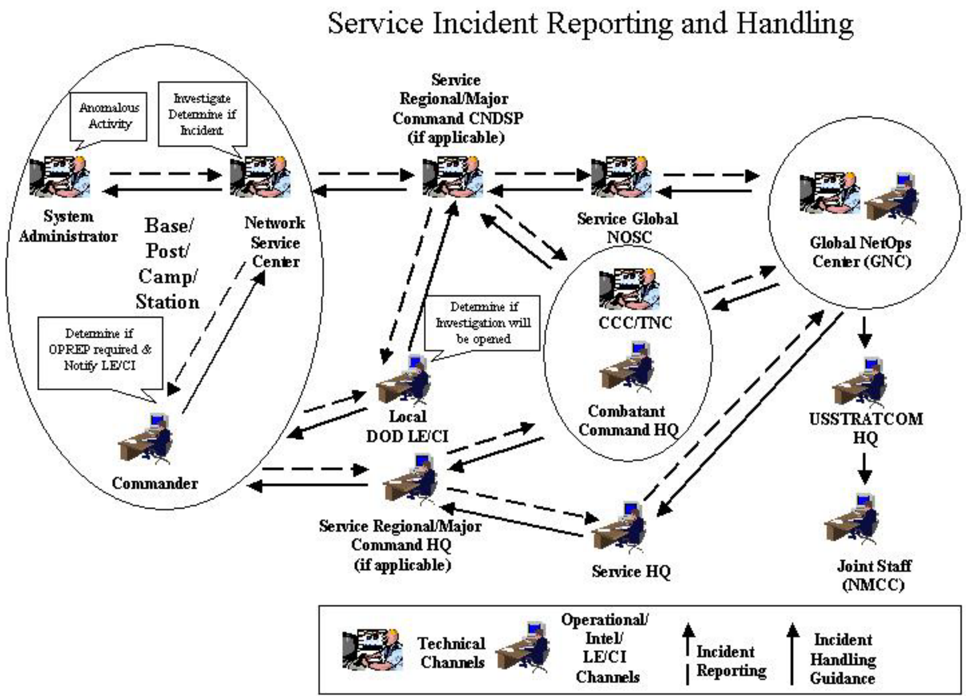

Service Incident Reporting and Handling
Anomalous Activity
Investigate Determine if Incident
System Administrator
Network Service Center
Base/ Post/ Camp/ Station
Determine if OPREP required & Notify LE/CI
Commander
Service Regional/Major Command CNDSP (if applicable)
Service Global NOSC
Global NetOps Center (GNC)
Determine if Investigation will be opened
Local DOD LE/CI
CCC/TNC
Combatant Command HQ
USSTRATCOM HQ
Service Regional/Major Command HQ (if applicable)
Service HQ
Joint Staff (NMCC)
Technical Channels
Operational/ Intel/ LE/CI Channels
Incident Reporting
Incident Handling Guidance

Figure B-B-C-1. Service Incident Reporting and Handling

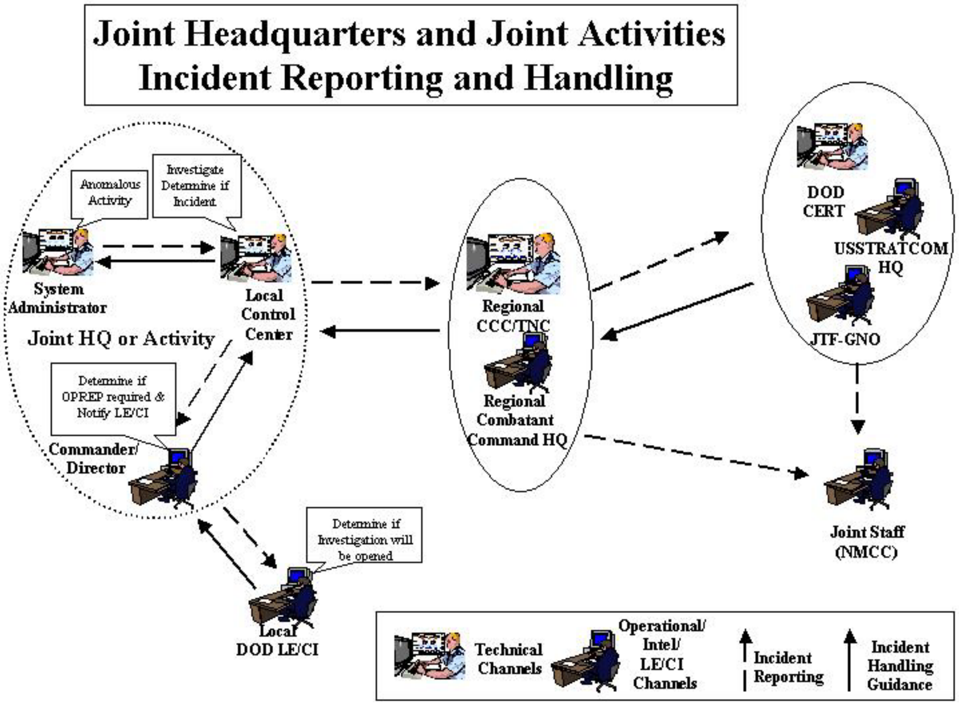

Joint Headquarters and Joint Activities Incident Reporting and Handling
Anomalous Activity
Investigate Determine if Incident
System Administrator
Local Control Center
Joint HQ or Activity
Determine if OPREP required & Notify LE/CI
Commander/ Director
Determine if Investigation will be opened
Local DOD LE/CI
Regional CCC/TNC
Regional Combatant Command HQ
DOD CERT
USSTRATCOM HQ
JTF-GNO
Joint Staff (NMCC)
Technical Channels
Operational/ Intel/ LE/CI Channels
Incident Reporting
Incident Handling Guidance

Figure B-B-C-2. Joint/Combatant Command Headquarters/Joint Activities Incident Reporting and Handling

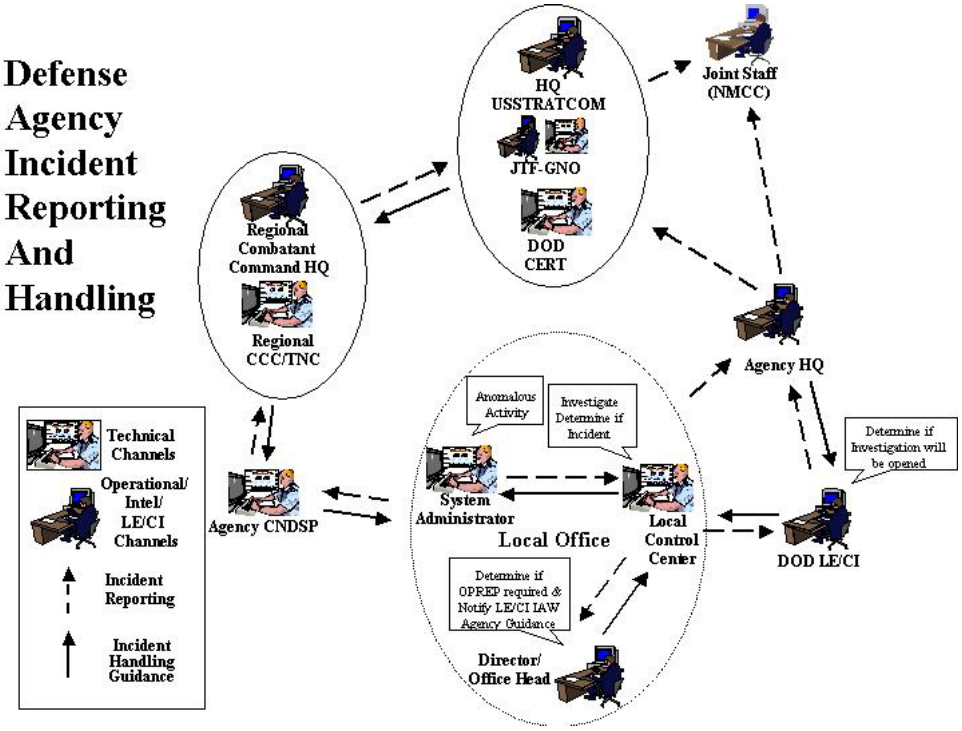

Defense Agency Incident Reporting And Handling
HQ USSTRATCOM
JTF-GNO
DOD CERT
Joint Staff (NMCC)
Regional Combatant Command HQ
Regional CCC/TNC
Agency HQ
Anomalous Activity
Investigate Determine if Incident
Determine if Investigation will be opened
Technical Channels
Operational/ Intel/ LE/CI Channels
Incident Reporting
Incident Handling Guidance
Agency CNDSP
System Administrator
Local Office
Local Control Center
DOD LE/CI
Determine if OPREP required & Notify LE/CI IAW Agency Guidance
Director/ Office Head

Figure B-B-C-3. Defense Agency Incident Reporting and Handling

7. Reporting Instructions

a. All C/S/As and field activities report incidents (or reportable events) affecting TS and below networks directly to the JTF-GNO or their CNDSP. All reportable events occurring across DOD SCI networks shall be reported via prescribed PAA authorities. The IC-IRC will ensure all TS/SCI reports are shared with JTF-GNO to ensure new vulnerabilities/exploits/incidents reported on compartmented systems are disseminated to administrators of affected systems through JTF-GNO Web site at http://www.jtfgno.smil.mil.

b. Organizations at all levels report changes in the status of reportable events, incidents, and incident-handling actions. Status reports are issued to the appropriate organizations when:

(1) There are changes in characteristics (e.g., increased/decreased activity; operational impact(s) on system, network or mission, etc.) of the reportable event or incident activity.

(2) Corrective actions are taken that change the status of the reportable event or incident activity.

(3) A reportable event or incident has been declared closed.

c. Tier 2 organizations report incidents to the JTF-GNO using Table B-B-B-1 as guide. Reminder, the JCD is the preferred method for reporting incidents. Organizations without SIPR access should report through their CNDSP, who enters the report into the JCD. Incidents may be entered through an automated database interface or through the JTF-GNO Web site.

d. CNDSP provide feedback to reporting organizations as information is developed. Subordinate echelons in the reporting chain are responsible for relaying information to the originating point and developing procedures to disseminate the information as appropriate within their constituent communities (NOSC, TNCC, or GNCC within the C/S/A or field activity and/or TNC within their area of responsibility (AOR)).

8. Report Format. There are two reporting formats. First, the general incident report format is used to report incidents and reportable events from the Tier 3 to Tier 2 levels. Second, the JCD reporting format, which can be found on the JCD Web site at http://jtidweb2.cert.smil.mil/jcd/, is used to report incidents and reportable events from Tier 2 to Tier 1 levels using the JCD.

a. The report format, Table B-B-C-1, is used for an initial report of incidents or reportable events. The following report format provides a structure for reporting initial incidents telephonically, by secure fax, or by other electronic means. Initial reports may be incomplete. Reporting organizations should balance the necessity of timely reporting (reports with critical information) versus complete reports (those with all blocks completed). Timely reporting is vital, and complete information should follow as details emerge.

b. In the initial report, the user provides as much information as possible. C/S/As and field activities may append to the report format to require more information for internal uses. As more information becomes available, provide additional detail in follow-on incident and reportable event reporting.

c. For a report to be considered “complete,” it contains, at a minimum, the information in Table B-B-C-1 below.

| Field | Description |
|---|---|
| CERT/CIRT Incident Number | Identify the reporting CERT/CIRT's reference number for tracking the incident. |
| Primary Incident Category | Identify access level gained as per Annex B Table B-1. |
| Secondary Incident Category | Identify any sub access level gained, if more than one category applies, as per Annex B Table B-1. |
| Attack Vector | Identify attack vector as per Annex B Table B-4. |
| Weakness | Identify system weakness as per Annex B Table B-5. |
| Last Update | ZULU date time group (DTG) of the last time the report was updated. Provide Year/Month/Day/Hour/Minute /Seconds. |
| Incident Start Date | ZULU DTG of the earliest event that was incorporated into the incident. Provide Year/Month/Day/Hour/Minute /Seconds. |
| Incident End Date | ZULU DTG that incident actually ended. Provide Year/Month/Day/Hour/Minute /Seconds. |
| Status | Status of the incident ("OPEN" or "CLOSED"). |
| System Classification | Report the Classification of the system under attack. "UNCLASSIFIED", "CONFIDENTIAL", "SECRET", "TOP SECRET", "SCI."<br>This field is NOT used to classify the reported incident. |
| Detecting Unit or Organization | Name of reporting unit or organization. |
| Affected Unit or Organization | Name of reporting affected unit or organization. |
| Action Taken | Indicates what action has been taken in response to the incident. Include notifications and associated reports. Include whether a copy of a medium was taken (image hard drives), or logs collected and disposition of mediums and logs). |
| Organization Tracking | Identify organization that is responsible for tracking the incident. |
| CERT Date Reported | ZULU DTG of when the incident was first reported to the CERT/CIRT. Provide year/month/day/hour/minute /seconds. |
| Operational Impact | Identify any detrimental effects on ability to perform mission by organization directly affected. Include organizations affected (e.g., due to being network users). Include impact on other organization(s) ability to perform mission. |
| Major Command | Based on owner of target IP address (e.g., USN, USAF, USSTRATCOM). |
| System Impact | This is a subjective field, but it is critical to get a general sense of the impact on operations of an incident. JTF-GNO provides additional guidance on how to better quantify operational impact. This is broken down into three grades. See Table C-2 for guidance. |
| Systems Affected | Number of systems affected by the incident. |

Table B-B-C-1. Incident and Reportable Event Report Format

| | |
|---|---|
| Staff Hours Lost | This is reported as an update record and may cause the impact field to be updated. Amount of time technical support is required to identify, isolate, mitigate, resolve, and recover from the attack and repair the attacked system (do not include analyst time spent analyzing the incident). |
| Exercise Name | Name of the exercise, if applicable. |
| Event Description | Provide a detailed description of the event, including what happened, how it occurred, and the current action taken to mitigate the event. |
| Source IP and port | Provide source IP with resolution data identifying owner and country of source IP machine. If the intruder is known, provide all identifying information to include objective of intruder, if known. (Source IP is not necessarily indicative of true origin). Footnote the source of resolution/attribution data – i.e., ARIN.org |
| Intruder(s) (if known) | Identify the intruder or group that is responsible for the incident, if known. |
| Origin (country) | Identify the source IPs country of origin. |
| Target IP(s) and port | Provide target IP with resolution identifying responsible command and physical location of target IP machine (B/C/P/S, etc.). Footnote the source of resolution/attribution data – i.e., DOD NIC, NSLOOKUP, WHOIS. If machine is behind a NAT'ed (network address translation enabled) router or firewall then also provide the wide area network (WAN) routable address (i.e. the Internet/SIPRNET routable IP address). |
| Technical Details | Provide a narrative description of the incident with technical details. Include DTGs of significant events (start, stop, or change of activity). State the use of the targeted system and whether the system is on- or off-line. Indicate whether the incident is ongoing. |
| Physical Location (base, camp, post, or station) | Identify the B/C/P/S that is affected by the intrusion and/or owns the target IP and where the physical system resides. |
| Technique, tool, or exploit used | Identify the technique, tool, or exploit that was used to exploit the vulnerability. |
| OS and version of OS | Record the operating system and version number of the operating system where the incident occurred. |
| Use of target (e.g., Web server, file server, host) | If applicable, for what the intruder/attacker used the target system for after it was exploited, if applicable. |
| DOD Network | Identifies network on which the incident occurred (e.g., NIPR or SIPR). |
| Comments | Provide amplifying information about the incident. |
| Synopsis | Provide an executive summary of the incident. |
| OPREP 3 Reporting | Identify if the incident was reported via OPREP 3 and what headquarters received the report. Attach a copy of the OPREP 3 report to this incident report, if applicable. |
| Contact Information: | Name: |

Table B-B-C-1. Incident and Reportable Event Report Format (cont.)

| | |
|---|---|
| | Organization: |
| | Telephone: |
| | Fax: |
| | E-mail: |

Table B-B-C-1. Incident and Reportable Event Report Format (cont.)

| Network Device | | CAT 1 | CAT 2 | CAT 3 | CAT 4 | CAT 5 | CAT 6 | CAT 7 |
|---|---|---|---|---|---|---|---|---|
| | Backbone | Severe | Severe | Minimal | Severe | Minimal | Minimal | Minimal |
| | Router | Severe | Severe | Minimal | Severe | Moderate | Minimal | Minimal |
| | Network Management/ Security Servers | Severe | Severe | Minimal | Severe | Moderate | Minimal | Moderate |
| | Non-Public Information Servers | Moderate | Moderate | Minimal | Moderate | Moderate | Minimal | Moderate |
| | Public Server | Minimal | Minimal | Minimal | Moderate | Minimal | Minimal | Moderate |
| | Work Station | Minimal | Minimal | Minimal | Moderate | Minimal | Minimal | Moderate |

Table B-B-C-2. System Impact Matrix

d. <u>Follow-on Report</u>. The incident report format (Table B-B-C-1) is used for all subsequent reports. Follow-on reports are submitted as directed by the higher CND organizations/ headquarters. If no direction is provided, follow-on reports are submitted within 8 hours of new information being developed about the incident. Additional reporting provides the raw details needed for the regional or global teams to understand the technical nature of the problem and is merged with information obtained from other reports to highlight regional or global trends. This report is forwarded IAW with table B-B-B-3.

e. The JTF-GNO provides timely feedback to reporting organizations, as more information becomes known. Feedback flows back through the incident reporting structure (Figures B-B-C-1 thru B-B-C-3). Subordinate layers in the reporting channels are responsible for relaying this information to the originating point and developing procedures to disseminate the information as appropriate within their constituent communities (NOSCs, TNCC, or GNCC within the C/S/A and field activity and/or TNC within their AOR). The format is also used by NOSCs or combatant command TNCCs and GNCCs and/or TNC organizations to report information developed through observation, correlation, analysis, or other means.

(1) Incident Criticality. This section identifies a list of questions to assist in determining the technical impact an incident. An incident criticality worksheet can be found at the JTF-GNO Web site.

a. Was this system fully patched and protected?

b. In the following timeframes, how many times has this exploit been used?

c. What system or network device does this exploit target?

d. What type of impact on DOD systems because of this compromise?

e. What access did the intruder need to successfully exploit the system?

f. To what extent did the attacker gain and escalate privileges?

g. How widespread is the compromise?

h. Are other DOD systems at risk because of this compromise?

i. How many DOD systems could be exploited in a similar fashion based on similar configurations?

j. Does the Department of Defense block port(s) associated with this exploit at the gateway?

k. What was the apparent intent of the compromise?

l. What level of information was affected?

8. Information Operations Condition (INFOCON). Commanders may raise INFOCON levels to re-establish the confidence level of systems based on the tradeoff in resources or execute tailored readiness options (TRO) to respond to specific intrusions or threats. Changes to INFOCON may require coordination with other C/S/As and field activities.

9. DOD Enterprise Incident Sets. Incident sets are groups of related incidents and associated data that require centralized management at the DOD level. Incident sets may span across multiple C/S/As and field

activities or merit DOD-level attention based on the scope or implications of the incidents. Due to the strategic concern and implications of incident sets, JTF-GNO should then notify STRATJIC IO Division of incidents and actions taken.

a. The JTF-GNO uses the reportable incidents and reportable events identified in Table B-B-B-1 (see Annex B) for consideration as DOD Enterprise incident sets.

b. The JTF-GNO is the central manager for all DOD Enterprise incident sets.

c. Incident sets are identified to the network operations community using CND tasking orders (CTOs), which designate:

(1) Incident set unique name.

(2) Summary description.

(3) POC information.

(4) Incident set signature indicators.

(5) Response action guidance for incidents meeting incident set criteria.

(6) Special reporting guidance for both technical reporting and operational reporting.

d. Tier 2 entities develop capabilities to track ongoing incident sets and determines if detected intrusions match criteria for inclusion.

e. Intrusions and/or alert data matching a defined incident set signatures are reported immediately to the JTF-GNO.

f. Coordination and deconfliction activities with the LE/CI community for JTF-GNO managed incident sets occur via the LE/CI Center at JTF-GNO.

11. DOD Protected Traffic List. The JTF-GNO maintains a DOD Protected Traffic List at http://www.jtfgno.smil.mil/Documents/ProtectedTraffic/ProtectedTraffic.doc to ensure critical DOD systems are not affected inadvertently by responses to CND events. This list includes Internet-NIPRNET traffic, enclave traffic, and key allied

interoperability traffic. This list includes technical data including IP addresses and transmission control protocol/Internet protocol (TCP/IP) ports, as well as operational impacts if protected traffic is blocked.

a. C/S/As and field activities notify the JTF-GNO of any actions taken that impact the DOD protected traffic list.

b. Systems on the DOD protected traffic list may be affected under extreme circumstances; therefore, it is imperative to identify the operational impact of actions taken prior to blocking traffic that may be on the protected traffic list.

12. DOD Network Deception Projects

a. DOD entities deploying network deception programs (e.g., honeypots) report the device and/or program to the JTF-GNO for situational awareness prior to connection to any DOD network. This information is used to deconflict sensor reports of suspicious activities or potentially vulnerable systems. Trusted agents within the JTF-GNO safeguard system information.

b. Information on deception projects include:

(1) Mission, intent, and purpose of the project.

(2) Location (internet address(es) and types of device(s)). This must include the WAN routable IP addresses.

(3) Type of data to be collected.

(4) POC for the device(s), to include telephone, e-mail, and organization.

13. Law Enforcement Practices. It is in the long-term interest of the Department of Defense to gain attribution and prosecute malicious individuals attacking DOD systems. The DOD CND community works hand in hand with the DOD LE/CI to investigate, track, and prosecute individuals who attack DOD systems.

a. The success of DOD CND response is dependent upon the Department of Defense’s ability to fuse information related to operations, service providers, law enforcement, counterintelligence, and intelligence assessment of the effects of network intrusions on the GIG.

b. Operational Cooperation with LE/CI

(1) In some circumstances LE/CI requests DOD system providers permit a potentially compromised DOD machine(s) remain operational (i.e., not disturbed in any way) to facilitate LE/CI investigations and operations. The commander of the organization should make every effort to support such requests; however, commanders are still required to maintain and defend their operations and subsequently, the networks that facilitate those operations.

(2) When investigative actions conflict with protective measures, these measures should be coordinated with the affected investigative service prior to taking these measures unless there is an imminent threat.

(3) Commanders must be careful to balance short-term requirement to conduct operations with the long-term advantage of prosecuting malicious individuals. If a commander is notified that legal process, such as a subpoena or warrant, has been issued and that their actions may conflict with the intent of that order, the commander should coordinate with LE/CI and the servicing Staff Judge Advocate (SJA) to coordinate any actions so that a legal process is not obstructed. Also promptly inform the JTF-GNO SJA of any potential conflict of this nature.

(4) Actions taken include but are not limited to copying device media to facilitate media analysis. Care should be taken in the release of device storage media images or the results of analysis. Media is classified to the highest level of information contained on the media. Additionally, the data on the media may be sensitive but unclassified, such as FOUO, limiting sharing outside the Department of Defense. Moreover, if the device is evidence in an LE/CI investigation, the media may be LE/CI sensitive, requiring special handling and a law enforcement sensitive (LES) caveat. While this does not forbid CND analysts from performing technical analysis, special care should be taken to ensure the dissemination of analytical results does not compromise a LE/CI investigation. The commander of the organization should coordinate with LE/CI when releasing such information. The operational community and LE/CI organizations must effectively collaborate in order to rapidly disseminate information necessary for network defense while minimizing the potential for compromise of LE/CI operations, sources, and methods. Many times this can be done effectively through the use of “tear lines,” etc.

c. LE/CI Threat Data. From a CND perspective, the principle value of the LE/CI community is the threat information it gleans through the course of conducting reactive and proactive investigations and operations. Threat data consists of information that can help lead to attribution and intent of network intruder(s) and can consist of planned actions that could adversely affect DOD systems. Threat data also consists of specific methodologies (toolsets, techniques, targeted vulnerabilities) used by network attackers that are discovered through the course of an investigation.

(1) Typical sources of data include:

(a) Logs and records of Internet service providers (ISP) recorded during the course of an intrusion, as well as those ISP records used to store hacking tools, stolen data, emails, chat rooms, etc.

(b) Liaison with local, state, federal, and international law enforcement counterparts.

(c) Recruitment of human sources in support of proactive operations and reactive investigations.

(d) Wiretaps, pen trap, and trace, etc.

(2) In addition to developing threat data through the course of an investigation or operation, the LE/CI community provides a means of deterrence through the enforcement of various statutes, and subsequent prosecution of those who violate the law. The CI community offers various capabilities and options when countering the activities of foreign intelligence services and international terrorists.

d. Insider Activity. LE/CI authorities and capabilities are typically the best option in addressing suspected and/or known access violations, theft, and damage caused by trusted insiders. Given “insiders” represent a large population (e.g., US military, GS civilians, contractors, and foreign national coalition partners), information related to potential insiders must always be handled very cautiously with respect to reporting.

e. Unique Restrictions on Law Enforcement Data. As noted above, the network defense can glean very important information from LE/CI investigation and/or operations; however, much of the information may require LES controls.

(1) To protect the operational security of ongoing investigative activity. When data is obtained via certain types of legal process, such as Title III wiretap orders, Foreign Intelligence Surveillance Act (FISA) orders, and grand jury subpoenas, it frequently has very strict controls on releasability. As one example, the results of grand jury subpoenas are very strictly controlled; unauthorized release of grand jury information can result in being held in contempt of court. However, there are procedures, promulgated in the USA Patriot Act that can be used to obtain grand jury information. A broad range of foreign intelligence or counterintelligence information may be released by an attorney for the government to other federal officials involved in, among other things, national defense, national security, and protective activities. Moreover, these procedures also permit the attorney for the government to disclose a matter involving the ability of the United States to protect against an actual or potential attack or other grave hostile acts by a foreign power, domestic terrorists, or international terrorists.

(2) There is the practical issue of establishing and maintaining trust among the numerous LE/CI agencies; although there may be no legal restriction on sharing certain information, say with respect to an ongoing operation, many agencies may be hesitant to share information that could jeopardize the safety of their sources, methods and agents. Although there are unique restrictions and considerations with regard to some of the information the LE/CI community obtains, if this information is important to the security of DOD systems, it can be shared with appropriate controls and limitations on distribution. To improve the flow and timeliness of the threat information obtained by the LE/CI community, both the DOD CND organizations, as well as the LE/CI community must ensure formalized processes are established to improve mutual understanding with respect to one another's needs, capabilities and unique restrictions.

15. International Coordination. There may be a need to coordinate quickly with the foreign nation in which attacking hosts reside or to determine that such a request is futile.

a. Key questions that may need to be addressed are:

(1) What is the state of relations between the United States and the nation in question?

(2) Will a request for assistance itself constitute a greater threat to national security than the attack or intrusion itself? This includes an assessment of whether the country is an actual sponsor of the attack or

may gain valuable information that could be used to harm the Department of Defense from future attacks.

(3) Does the nation in question have the technical capacity to respond to a request for assistance?

(4) How long will it take for the nation to act on the request? Is that too long given the threat to national security?

b. LE/CI organizations have a long history of working with their counterparts in certain foreign countries. These relationships should be utilized to the greatest extent practicable according to the extent to which they may be beneficial. The LE/CI Center at JTF-GNO shall serve as the repository for relevant information shared by the LE/CI community, conveying CND organization requests for information to the LE/CI community and providing a focal point for LE/CI coordination with JTF-GNO. In cases where international coordination is required beyond the capabilities of the LE/CI community, CDRUSSTRATCOM shall forward a request to the US Department of State via the Secretary of Defense.

(INTENTIONALLY BLANK)

## ANNEX D TO APPENDIX B TO ENCLOSURE B

## CND INCIDENT HANDLING TOOLS

1. This annex provides an overview of common tools that are used by the CND community to facilitate incident handling.

2. User Defined Operational Picture (UDOP). The CND UDOP provides local, intermediate, and DOD-wide situational awareness of CND activities, operations, and their impact. The Enterprise Sensor Grid (ESG) feeds the UDOP. The ESG collects, processes, and stores the DOD networking sensing environment, (e.g., raw, processed, correlated, alert, etc.) available for use by the CND analyst. The CND UDOP will provide an Enterprise view of the C/S/A and field activity sensors, vulnerabilities, and protection capabilities. The UDOP leverages common data, views, and mechanisms for data sharing. It provides information to the CND analyst community that facilitates the execution of selected COAs to mitigate and respond to attacks directed at the GIG.

3. Joint CERT Database (JCD). The JCD is an automated repository of all computer reportable events and incidents in the Department of Defense.

a. It is intended to be the primary reporting mechanism of actionable computer network reportable events and incidents to the JTF-GNO and is the basis for JTF-GNO support to combatant commanders, senior government leaders, and civilian authorities.

b. The C/S/As and field activities provide reportable event and incident reports to the JCD in the form of database records.

c. These reportable event and incident records are integrated, correlated, and displayed using a variety of visualization applications, the combination of which provide the CND community with a shared situational awareness capability.

d. The JTF-GNO is the functional owner of the JCD. The JTF-GNO maintains and manages the JCD. Access to the JCD can be obtained through JTF-GNO on the SIPRNET.

(INTENTIONALLY BLANK)

## ANNEX E TO APPENDIX B TO ENCLOSURE B

## INTELLIGENCE SUPPORT TO INCIDENT REPORTING

1. Phased Reporting Procedures

a. CND intelligence reporting on network events focuses on foreign threats to DOD networks and has been divided into three phases.

(1) A Phase I intelligence report is generated in a timely manner for events meeting a specified reporting threshold, based on technical event data augmented with all-source intelligence information.

(2) A Phase II intelligence report is also an all-source report and can be a correlation of Phase I reporting.

(3) A Phase III intelligence report is an all-source finished intelligence product intended for a general audience.

b. The primary CND intelligence analysis tool suite used to derive phased intelligence reporting is the Joint Threat Incident Database (JTID) and the Joint Threat Intelligence Portal (JTIP).

c. Individual entries in the JTID are referred to as Threat Incident Database records (TID) and are based on threat activity against DOD networks that might be of foreign origin.

d. Use of the JTID for recording possible foreign and domestic threat activity against DOD networks is required by the JTF-GNO J-2 and each Service Component CERT/CIRT intelligence support element for Category 1 – Root Level Intrusion, 2 – User Level Intrusion, 4 - DOS, 6 – Reconnaissance (determined to be significant), and 8 – Investigating reportable events and incidents that appear to be associated with USSTRATCOM/JTF-GNO focused operations. The JTID is populated with TIDs based on JCD entries corresponding to threat activity against DOD computers and networks. TIDs include both technical and intelligence data related to the IP addresses conducting activity against DOD systems.

e. The objective of phased intelligence reporting is to share intelligence information and events in support of CND to enable rapid cross-cueing of threat activity and fusion of all-sources of information on foreign threats to DOD networks.

2. Phase I Intelligence Reports. Phase I intelligence reports are referred to as Phase I Network Intelligence Reports (NIRs).

a. Phase I NIRs contain a technical summary of an event supplemented with intelligence analysis and are written for the operational community. Technical event details are derived from an entry in the JCD. Technical specificity in Phase I reporting is vital to establishing or ruling out correlation between events during Phase II analysis.

b. A Phase I NIR is required for every Category 1 – Root Level Intrusion, 2 – User Level Intrusion, 4 - DOS, 6 – Reconnaissance, and 8 – Investigating reportable events and incidents that appear to be associated with USSTRATCOM/JTF-GNO focused operations. Compilation NIRs or NIRs that address several obviously related Category 1, 2, 4, and 6 incidents and reportable events occurring at or near the same time period are permissible.

c. Phase I NIRs are required to be reported within 48 hours of recognition that an event meets one of the above categories. Supplemental Phase I NIRs will be produced as additional information becomes available.

d. The JTF-GNO J-2 and the Service Component CERT/CIRT intelligence support elements are required to perform Phase I reporting.

e. Phase I NIRs will be written for release to allies as much as possible.

f. Phase I NIRs will follow the format and content as promulgated by the JTF-GNO J-2.

3. Phase II Intelligence Reports. Phase II intelligence reports are referred to as Phase II reports and contain standard types of information but allow for flexibility in formatting. Phase II reports can be based upon patterns that emerge from correlation of Phase I NIRs. There are generally two types of correlation under Phase II reporting: event-based and entity-based reporting.

a. As with Phase I reporting, timeliness for Phase II reporting is important. Upon recognition of a pattern of malicious network activity, a Phase II report is required within 72 hours.

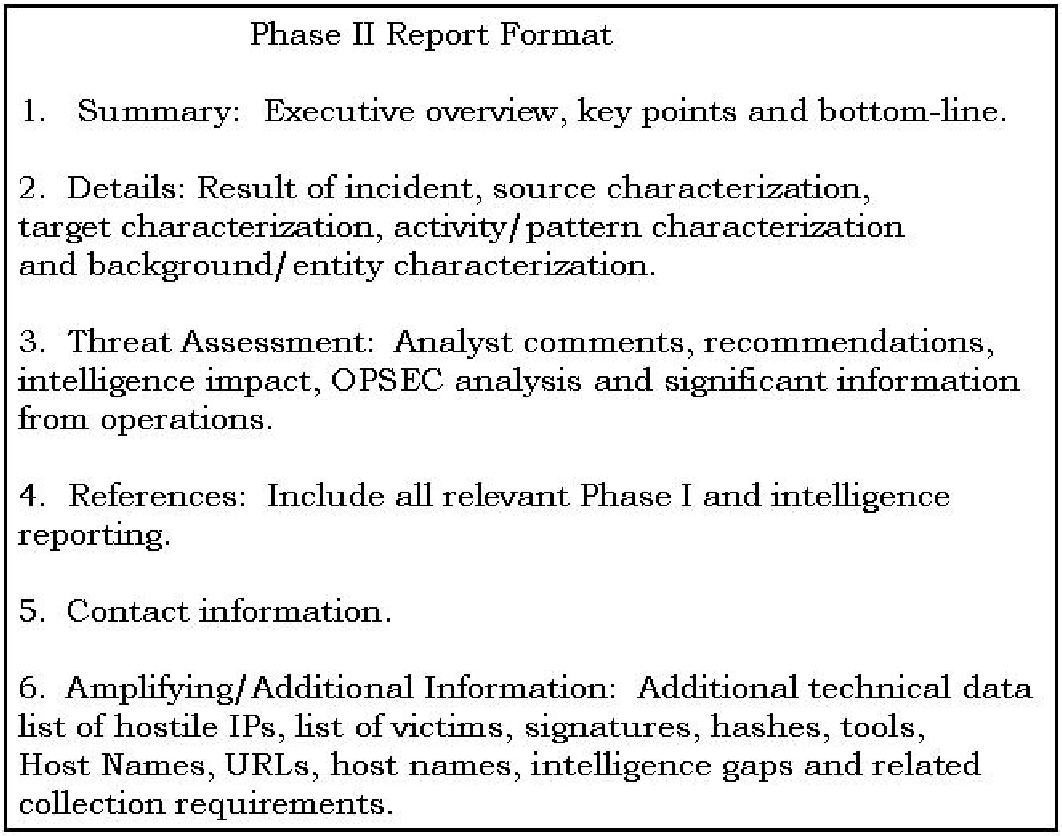
(1) Initial Phase II reports will be disseminated through message traffic with a URL link to the report if appropriate.

(2) Phase II reports will have a standard Title/Subject line. Example: "CND Phase II Report: Title, Service/Organization"

b. The JTF-GNO J-2 and the Service Component Command CERT/CIRT intelligence support elements are required to perform Phase II reporting. Phase II reporting may also be generated by Combatant Command Joint Intelligence Centers/Joint Analysis Center (JICs/JAC), DIA, NSA, and Service intelligence centers.

c. Phase II reports will be written for release to allies as much as possible.

d. Phase II reports will be in following format (Table B-B-E-1):



Phase II Report Format

1. Summary: Executive overview, key points and bottom-line.

2. Details: Result of incident, source characterization, target characterization, activity/pattern characterization and background/entity characterization.

3. Threat Assessment: Analyst comments, recommendations, intelligence impact, OPSEC analysis and significant information from operations.

4. References: Include all relevant Phase I and intelligence reporting.

5. Contact information.

6. Amplifying/Additional Information: Additional technical data list of hostile IPs, list of victims, signatures, hashes, tools, Host Names, URLs, host names, intelligence gaps and related collection requirements.

Table B-B-E-1. Phase II Report Format

4. Phase III Intelligence Reports. Phase III intelligence reports is an all-source finished intelligence report for a general audience.

a. The objectives of Phase III reports are:

(1) Determine final attribution.

(2) Provide full-scope examinations of events and incidents.

(3) Provide assessment of event and incident strategic significance.

(4) Provide damage assessments.

b. Phase III reports may omit the depth of details provided in Phase I NIRs or Phase II reports. There is a higher standard of certainty and depth for Phase III reporting than Phase II reports. These reports should attempt to capture the full military and/or political significance of network activity. Phase III reporting is normally generated in response to intelligence consumer production requirements based on their production priorities and focus.

c. Phase III reports may be based upon a wide variety of reporting topics relevant to events, incidents, entities or issues. Phase III reports can be oriented on providing additional depth and significance regarding existing Phase I or II reporting about network events or incidents but may also not be relate to specific network events or incidents. For example, these reports may provide potential threat information on foreign actors (e.g., governments, sub-national actors, individuals), technology issues or trends, future projections, case studies, or global characterizations.

d. Timeliness for Phase III reporting is an important consideration because it must be relevant to operational needs and other consumer requirements. Although it is not possible to designate a specific time requirement, once a consumer deadline has been established, the intelligence production element must meet that requirement on a timely basis.

e. Phase III reports may be generated by any CND intelligence provider.

f. Formatting for Phase III reports is flexible; however, generally Phase III reports will conform to DOD-wide standards such as the Defense Analysis Reports.

## ENCLOSURE D

## REFERENCES

a. DOD 5200.2-R Series, “Personnel Security Program”

b. CJCSI 6510.01 Series, “Information Assurance (IA) and Computer Network Defense (CND)”

c. CJCSI 6211.02 Series, “Defense Information System Network (DISN): Policy, Responsibilities and Processes”

d. DOD Directive 5200.39, 10 September 1997, “Security, Intelligence and Counterintelligence Support to Acquisition Program Protection”

e. NSTISSI No. 7003, 13 December 1996, “Protected Distribution System”

f. DOD Instruction 5200.40, 30 December 1997, “DOD Information Technology Security Certification and Accreditation (C&A) Process”

g. DOD Instruction O-8530.2 Series, “Support to Computer Network Defense (CND)”

h. Executive Order 12958, 17 April 1995, “Classified National Security Information”

i. DOD 5200.1-R, 14 January 1997, “Information Security Program”

j. DOD 5500.7-R Change 4, 6 August 1998, “Joint Ethics Regulation”

k. USD(P&R) and ASD(C3I) memorandum, 29 June 1998, “Information Assurance (IA) Training and Certification”

l. NSTISSD No. 500, 25 February 1993, “Information Systems Security (INFOSEC) Education, Training, and Awareness”

m. NSTISSD No. 501, 16 November 1992, “National Training Program for Information Systems Security (INFOSEC) Professionals”

n. CNSSI No. 4013, March 2004, “National Information Assurance Training Standard For System Administrators”

o. National Institute of Standards and Technology (NIST) Special Publication 800-16, April 1998, “Information Technology Security Training Requirements”

p. CNSSI No. 4014, April 2004, “Information Assurance Training Standard For Information Systems Security Officers”

q. CNSSI No. 4012, June 2004, “National Information Assurance Training Standard For Senior Systems Managers”

r. CJCSI 3401.01 Series, “Chairman’s Readiness System”

s. DOD Directive O-8530.1 Series, “Computer Network Defense (CND)”

t. NSTISSD No. 503, 30 August 1993, “Incident Response and Vulnerability Reporting for National Security Systems Security”

u. DOD Instruction O-3600.2 Series, “Information Operations (IO) Security Classification Guidance”

v. DOD Directive 5105.61, 3 May 1997, “DOD Cover and Cover Support Activities”

w. DOD Instruction 8500.2 Series, “Information Assurance (IA) Implementation”

x. DI-2710-6-01, January 2001, “The Information Operations Threat To The Defense Information Systems Network (DISN)”

y. National Disclosure Policy (NDP-1), 1 October 1988, “National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations”

z. DOD Directive 5230.11, 16 June 1992, “Disclosure of Classified Military Information to Foreign Governments and International Organizations”

aa. DOD Directive 5230.20 Series, “Visits and Assignment of Foreign Nationals”

bb. DOD Directive 5230.25, 6 November 1984, “Withholding of Unclassified Technical Data from Public Disclosure”

cc. DOD Instruction 5230.17, 17 August 1979, , “Procedures and Standards for the Disclosure of Military Information to Foreign Activities”

dd. CJCSI 5221.01 Series, “Delegation of Authority to Commanders of Combatant Commands to Disclose Classified Military Information to Foreign Governments and International Organizations” ee. CJCSI 6740.01 Series, “Military Telecommunications Agreements and Arrangements between the United States and Regional Defense Organizations or Friendly Nations”

ff. Title 22, Code of Federal Regulations, Parts 120-130, “International Traffic in Arms Regulations (ITAR)”

gg. Title 15, Code of Federal Regulations, Parts 730-799, “Export Administration Regulations (EAR)”

hh. DOD Directive 5400.7, Change 1, 17 June 2002, “DOD Freedom of Information Act Program”

ii. FIPS 10-4, April 1995, “Countries, Dependencies, Areas Of Special Sovereignty, And Their Principal Administrative Divisions”

jj. Title 10, United States Code, section 421

kk. NSTISSP No. 8, 13 February 1997, “National Policy Governing the Release of Information Systems Security (INFOSEC) Products or Associated INFOSEC Information to Foreign Governments”

ll. DOD Instruction S-5225.1, Change 1, 16 November 1994, “Communications Security (COMSEC) Assistance to Foreign Governments and International Organizations”

mm. CJCSI 6510.06 Series, “Communications Security Releases to Foreign Nations”

nn. DOD Directive C-5200.5, 21 April 1990, “Communications Security (COMSEC)”

oo. Public Law 100-235, 8 January 1988, “Computer Security Act of 1987”

pp. NSTISSAM INFOSEC 1-00, 8 February 2000, “Advisory Memorandum For The Use Of The Federal Information Processing Standards (FIPS) 140-1 Validated Cryptographic Modules In Protecting Unclassified National Security Systems”

qq. OMB Circular No. A-130, 28 November 2000, “Management of Federal Information Resources”

rr. CNSSP-1, September 2004, “National Policy For Safeguarding And Control of Communications Security Material” ss. CNSSP-14, November 2002, “Governing The Release Of Information Assurance (IA) Products To Authorized U.S. Persons Or Activities That Are Not Part Of Federal Government”

tt. DOD Directive 4640.6, 26 June 1981, “Communications Security (COMSEC) Monitoring and Recording”

uu. NTISSD No. 600, 10 April 1990, “Communications Security (COMSEC) Monitoring”

vv. NSTISSP No. 3, 19 December 1988, “National Policy for Granting Access to US Classified Cryptographic Information”

ww. Executive Order 12333, 4 December 1981, “United States Intelligence Activities”

xx. ASD(C3I) memorandum, 16 January 1997, “Policy on Department of Defense Electronic Notice and Consent Banner”

yy. Title 10, United States Code, section 2315

zz. Title 15, United States Code, section 278g-3

aaa. FIPS 140-2, 25 May 2001, “Security Requirements for Cryptographic Modules”

bbb. DOD Directive 8500.1, Series, “Information Assurance (IA)”

ccc. DOD 8510.1-M, July 2000, “Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual”

ddd. Intelligence Community CIO, TOP SECRET/Sensitive Compartmented Information (SCI) and Below Interoperability Policy (TSABI)”

eee. Director of Central Intelligence Directive (DCID) 6/3, Administratively Updated, 3 May 2002, “Protecting Sensitive Compartmented Information within Information Systems”

fff. National Security Agency, Series, “Department of Defense Firewall Guidance”

ggg. DOD PKI Program Management Office, 9 February 2005, “X.509 Certificate Policy for the United States Department of Defense” hhh. CNSSI No. 4009, May 2004, “National Information Assurance (IA) Glossary”

iii. Joint Publication 1-02, as amended through 31 August 2005, “Department of Defense Dictionary of Military and Associated Terms”

jjj. Federal Standard 1037C, 7 August 1996, “Telecommunications: Glossary of Telecommunications Terms”

kkk. Joint Publication 3-13, 13 February 2006, “Joint Doctrine for Information Operations”

lll. Federal Information Security Management Act (FISMA) of 2002

mmm. ASD (C3I) memorandum, 26 February 2003, “Guidance for Computer Network Defense Response Actions.”

nnn. CJCSM 3150.03B Series, “Joint Reporting Structure Event and Incident Reports”

ooo. Title 18, United States Code, section 2511(2)(a)(i)).

ppp Strategic Command Directive (SD) 527-1, 27 January 2006, “Department of Defense (DOD) Information Operations Condition (INFOCON) System Procedures"

(INTENTIONALLY BLANK)

# GLOSSARY

## PART I--ABBREVIATIONS AND ACRONYMS

| | |
|---|---|
| ACL | access control list |
| ACERT | US Army computer emergency response team |
| AFCERT | US Air Force computer emergency response team |
| AOR | area of responsibility |
| ASD(C3I) | Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) |
| ASD(NII) | Assistant Secretary of Defense (Network and Information Integration) |
| AUTODIN | automated digital network |
| AV | anti-virus |
| | |
| BDA | battle damage assessment |
| B/P/C/S | base/post/camp/station |
| | |
| C2 | command and control |
| CA | certification authority |
| CC | common criteria |
| CCC-K | C4 Control Center-Korea |
| CCII | commander's critical items of information |
| CCIR | Commander’s Critical Information Requirements |
| CDRUSSTRATCOM | Commander, United States Strategic Command |
| CENTRIXS | Combined Enterprise Regional Information Exchange System |
| CERT | computer emergency response team |
| CI | counterintelligence |
| CIO | chief information officer |
| CIRT | computer incident response team |
| CJCS | Chairman of the Joint Chiefs of Staff |
| CJCSI | Chairman of the Joint Chiefs of Staff Instruction |
| CJCSM | Chairman of the Joint Chiefs of Staff Manual |
| CL | compliance level |
| CM | configuration management |
| CMA | certificate management authority |
| CMCS | communications security (COMSEC) material control system |
| CNA | computer network attack |
| CND | computer network defense |
| CND RA | CND Response Action |
| CNDSP | Computer Network Defense Service Provider |
| CNE | computer network exploitation |
| CNSS | Committee on National Security Systems |

| | |
|---|---|
| COE | common operating environment |
| COMSEC | communications security |
| CONOPS | concept of operations |
| COTS | commercial-off-the-shelf |
| CPMWG | Certificate Policy Management Working Group |
| CPS | certification practice statement |
| C/S/A | combatant command, Service and/or agency |
| CTO | CND tasking order |
| CWAN | coalition wide area network |

| | |
|---|---|
| D&D | denial and deception |
| DAA | designated approving authority |
| DCID | Director of Central Intelligence Directive |
| DCIOS | Defense Criminal Investigative Organizations |
| DCOG | Defense Cyber Operations Group |
| DECC | Defense Enterprise Computing Center |
| DES | data encryption standard |
| DHS | Department of Homeland Security |
| DIA | Defense Intelligence Agency |
| DICAST | Defense and Intelligence Community Accreditation Support Team |
| DII | defense information infrastructure |
| DIRNSA | Director, National Security Agency |
| DISA | Defense Information Systems Agency |
| DISN | Defense Information System Network |
| DITSCAP | DOD Information Technology Security Certification and Accreditation Process |
| DMS | Defense Message System |
| DMZ | demilitarized zone |
| DNS | domain name system |
| DOD | Department of Defense |
| DODD | Department of Defense Directive |
| DODI | Department of Defense Instruction |
| DOS | denial of service |
| DSAWG | DISN Security Accreditation Working Group |
| DSN | Defense Switched Network |
| DTG | date time group |

| | |
|---|---|
| EA | electronic attack |
| EAL | evaluation assurance level |
| EAR | export administration regulations |
| EO | executive order |
| EP | electronic protection |
| ESG | Enterprise Sensor Grid |
| EW | electronic warfare |

| | |
|---|---|
| FDO | foreign disclosure officer |
| FIPS | federal information processing standard |
| FISA | Federal Intelligence Surveillance Act |
| FISMA | Federal Information Security Management Act of 2002 |
| FLO | foreign liaison officer |
| FMS | foreign military sales |
| FOUO | FOR OFFICIAL USE ONLY |
| FTP | file transfer protocol |
| | |
| GCCS | Global Command and Control System |
| GCSS | Global Combat Support System |
| GIAP | Global Information Grid (GIG) interconnection approval process |
| GIG | Global Information Grid |
| GNCC | Global Network Control Center |
| GNOSC | Global Network Operations and Security Center |
| GNSC | Global NetOps Support Center |
| GSO | guarding solutions office |
| GTLD | Generic Top Level Domain |
| | |
| HTML | hypertext markup language |
| | |
| I&W | indications and warning |
| IA | information assurance |
| IAIP | Information Assurance Infrastructure Protection |
| IAM | information assurance manager |
| IAO | information assurance officer |
| IAPC | Information Assurance Protection Center |
| IATF | information assurance technical framework |
| IATO | interim authority to operate |
| IAVA | information assurance vulnerability alert |
| IAVB | information assurance vulnerability bulletin |
| IAVM | information assurance vulnerability management |
| IAW | in accordance with |
| IC | Intelligence Community |
| IC-IRC | Intelligence Community Incident Response Center |
| ID | identification |
| IDS | intrusion detection system |
| INFOCON | information operations conditions |
| INFOSEC | information systems security |
| INMS | integrated network management system |
| IO | information operations |
| IP | Internet protocol |

| | |
|---|---|
| IPC | information protection cell |
| IPSec | Internet protocol security |
| ISP | Internet service provider |
| ISSM | information systems security manager |
| ISSO | information systems security officer |
| IT | information technology |
| ITAR | international traffic in arms regulations |
| IW | information warfare |
| J-3 | operations directorate of a joint staff |
| J-6 | command, control, communications, and computer systems directorate of a joint staff |
| JCD | Joint CERT Database |
| JCMA | Joint Communications Security (COMSEC) Monitoring Activity |
| JFCC | Joint Functional Component Command |
| JP | joint publication |
| JTF | joint task force |
| JTF-CNO | Joint Task Force - Computer Network Operations |
| JTF-GNO | Joint Task Force - Global Network Operations |
| JTID | Joint Threat Incident Database |
| JTIP | Joint Threat Intelligence Portal |
| JULLS | Joint Universal Lessons-Learned System |
| JVAP | joint vulnerability assessment process |
| JWICS | Joint Worldwide Intelligence Communications System |
| LAN | local area network |
| LCC | local control center |
| LE/CI | Law Enforcement/Counter Intelligence |
| LES | law enforcement sensitive |
| LRA | local registration authority |
| MAC | mission assurance category |
| MARCERT | US Marine Corps computer emergency response team |
| MB | megabyte |
| MNIS | Multinational Information Sharing |
| MOA | memorandum of agreement |
| MOU | memorandum of understanding |
| MS-DOS | Microsoft Disk Operating System |
| NAT | network address translation |
| NAT’ed | network address translation enabled |
| NAVCIRT | US Navy computer incident response team |

| | |
|---|---|
| NCC | network control center |
| NCSC | National Communications Security Committee |
| NDP | national disclosure policy |
| NetOps | network operations |
| NGA | National Geospatial-Intelligence Agency |
| NIAP | national information assurance partnership |
| NIC | network interface cards |
| NIPC | National Infrastructure Protection Center |
| NIPRNET | Non-classified Internet Protocol Router Network |
| NIR | Network Intelligence Report |
| NIST | National Institute of Standards and Technology |
| NOSC | Network Operations and Security Center |
| NRO | National Reconnaissance Office |
| NSA | National Security Agency |
| NSC | Network Service Center |
| NSIRC | National Security Incident Response Center |
| NSISIP | National Security Information Systems Incident Program |
| NSTISSC | National Security Telecommunications and Information Systems Security Committee |
| NSTISSD | National Security Telecommunications and Information Systems Security Directive |
| NSTISSI | National Security Telecommunications and Information Systems Security Instruction |
| NSTISSAM | National Security Telecommunications and Information Systems Security Advisory Memorandum |
| NSTISSP | National Security Telecommunications and Information Systems Security Policy |
| | |
| OCA | original classification authority |
| OCIN | organization's classified information network |
| OI | operational impact |
| OMB | Office of Management and Budget |
| OPR | office of primary responsibility |
| OPREP | operational report |
| OPSEC | operations security |
| OS | operating system |
| OSI | open systems interconnection |
| OUNET | organization's unclassified network |
| | |
| PAA | principal accrediting authority |
| PDS | protected distribution system |
| PIN | personal identification number |
| PKI | public key infrastructure |
| PM | program manager |

| | |
|---|---|
| PMA | policy management authority |
| PNA | protection for the network |
| POA&M | plan of action and milestones |
| POC | point of contact |
| PSYOP | psychological operations |
| | |
| QoS | quality of service |
| | |
| RA | release authority |
| RASP | remote access security program |
| RCERT | regional computer emergency response team |
| RDT&E | research, development, test, and evaluation |
| RF | radio frequency |
| RHR | reliable human review |
| RI | referenced implementation |
| RNOSC | regional network operations and security center |
| RTO | request to operate |
| | |
| SA | system administrator |
| SABI | SECRET and Below Interoperability |
| SBU | sensitive but unclassified |
| SCAO | SIPRNET Connection Approval Office |
| SCI | sensitive compartmented information |
| SIPRNET | SECRET Internet Protocol Router Network |
| SIGINT | signals intelligence |
| SJA | Staff Judge Advocate |
| SLA | service-level agreement |
| S/MIME | secure multipurpose Internet mail extension |
| SMTP | simple message transfer protocol |
| SOP | standing operating procedure |
| SRR | security readiness review |
| SSAA | system security authorization agreement |
| SSES | system security engineering survey |
| SSH | secure socket shell |
| SSL | secure sockets layer |
| SSN | social security number |
| STIG | security technical implementation guide |
| SYN | synchronous idle character |
| | |
| TA | technical advisory |
| TBP | to be published |
| TCCC | Theater C4I Control Center |
| TCP | transmission control protocol |
| TDY | temporary duty |
| TI | technical impact |
| TID | Threat Incident Database Records |

| | |
|---|---|
| TIG | Theater Information Grid |
| TLS | transport layer security |
| TNC | Theater NetOps Center |
| TNCC | Theater Network Control Center |
| TPFDD | time-phased force deployment data |
| TRO | tailored readiness option |
| TSABI | TOP SECRET/SCI and Below Interoperability |
| | |
| UCMJ | Uniform Code of Military Justice |
| UDOP | User Defined Operational Picture |
| UNIX | universal interactive executive |
| URL | universal resource locator |
| US CERT | US Computer Emergency Response Team |
| USD(P&R) | Under Secretary of Defense for Personnel and Readiness |
| USG | United States Government |
| USSTRATCOM | United States Strategic Command |
| | |
| VAT | vulnerability assessment team |
| VCTS | vulnerability compliance tracking system |
| VMS | vulnerability management system |
| VPN | virtual private networks |
| | |
| WA | Web application |
| WAN | wide area network |
| WMD | weapons of mass destruction |
| WSH | windows scripting host |
| | |
| ZULU | time zone indicator for Universal Time |

(INTENTIONALLY BLANK)

## GLOSSARY

## PART II--DEFINITIONS

access. The opportunity to make use of an information system resource. (CNSS Instruction No. 4009)

access control. Limiting access to information system resources only to authorized users, programs, processes, or other systems. (CNSS Instruction No. 4009)

accountability. Process of tracing information system activities to a responsible source. (CNSS Instruction No. 4009)

accreditation. Formal declaration by a designated approving authority that an information system is approved to operate in a particular security mode at an acceptable level of risk, based on implementation of an approved set of technical, managerial, and procedural safeguards. (CNSS Instruction No. 4009)

action. A step taken by a user or process in order to achieve a result, such as to probe, scan, flood, authenticate, bypass, spoof, read, copy, steal, modify, or delete. (CJCSI 6510.01)

application. Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges. Examples include office automation, electronic mail, Web services, and major functional or mission software programs. (DODD 8500.1)

architecture. The configuration of any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Includes computers, ancillary equipment, and services, including support services and related resources. (DODI 5200.40)

asset. Any device on any DOD-owned or controlled information system network, to include but not limited to workstations, servers, routing devices (router, switch, firewall), networked peripherals (e.g., network printers) and guards. The device is considered a single node on a network, such that it has its own network identification (Internet protocol and/or media access control address). (CJCSM 6510.01)

audit. Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. (CNSS Instruction No. 4009)

audit trail. Chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event. (CNSS Instruction No. 4009)

authentication. 1. A security measure designed to protect a communications system against acceptance of a fraudulent transmission or simulation by establishing the validity of a transmission, message, or originator. 2. A means of identifying individuals and verifying their eligibility to receive specific categories of information. 3. Evidence by proper signature or seal that a document is genuine and official. 4. In evasion and recovery operations, the process whereby the identity of an evader is confirmed. (Joint Publication (JP) 1-02)

availability. Timely, reliable access to data and information services for authorized users. (CNSS Instruction No. 4009)

backup. Copy of files and programs made to facilitate recovery, if necessary. (CNSS Instruction No. 4009)

Blue Team. Cooperative effort by an interdisciplinary team to review, assess, and document vulnerabilities as a means to improve the security posture of information systems. (CJCSM 6510.01)

category. Restrictive label applied to classified or unclassified information to limit access. (CNSS Instruction No. 4009)

certification. Comprehensive evaluation of the technical and nontechnical security features of an information system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements. (CNSS Instruction No. 4009)

classified information. Official information that has been determined to require, in the interests of national security, protection against unauthorized disclosure and which has been so designated. (JP 1-02)

command and control system. The facilities, equipment, communications, procedures, and personnel essential to a commander for planning, directing, and controlling operations of assigned forces pursuant to the missions assigned. (JP 1-02)

Command Communications Service Designators. An eight character alphanumeric that is used to identify the circuit throughout the joint communications network. (CJCSM 6510.01)

common operating environment (COE). The collection of standards, specifications and guidelines, architecture definitions, software infrastructures, reusable components, application programming interfaces, runtime environment definitions, reference implementations, and methodology that establishes an environment on which a system can be built. The COE is the vehicle that assures interoperability through a reference implementation that provides identical implementation of common functions. It is important to realize that the COE is both a standard and an actual product. (CJCSM 6510.01)

communications security. The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. Communications security includes: cryptosecurity, transmission security, emission security, and physical security of COMSEC materials and information. a. **crypto-security** — The component of communications security that results from the provision of technically sound cryptosystems and their proper use. b. **transmission security** — The component of communications security that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptoanalysis. c. **emission security** — The component of communications security that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from cryptoequipment and telecommunications systems. d. **physical security** — The component of communications security that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. (JP 1-02)

communications security monitoring. The act of listening to, copying, or recording transmissions of one's own official telecommunications, including voice and data, to provide material for analysis in order to determine the degree of security being provided to those transmissions. (modified from National Security Telecommunications and Information System Security Directive (NTISSD) No. 600)

community risk. Probability that a particular vulnerability will be exploited within an interacting population and adversely impact some members of that population. (DODD 8500.1) computer emergency response team(s). Computer emergency response teams (CERTs) are teams composed of personnel with technical expertise and organic equipment that may deploy to assist remote sites in the restoration of computer services. Services have formed CERTs as an operational organization for rapid response to both deployed and installation based Service forces. (JP 3-13) Note: CERT is an organization chartered by an information systems owner to coordinate or accomplish necessary actions in response to computer emergency incidents that threaten the availability or integrity of its information systems.

computer network attack. Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (JP 1-02)

computer network exploitation. Intelligence collection operations that obtain information resident in files of threat automated information systems (AIS) and gain information about potential vulnerabilities, or access critical information resident within foreign AIS that could be used to the benefit of friendly operations. (CJCSI 6510.01)

computer network defense (CND). Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks. NOTE: The unauthorized activity may include disruption, denial, degradation, destruction, exploitation, or access to computer networks, information systems or their contents, or theft of information. CND protection activity employs information assurance protection activity and includes deliberate actions taken to modify an assurance configuration or condition in response to a CND alert or threat information. Monitoring, analysis, and detection activities, including trend and pattern analysis, are performed by multiple disciplines within the Department of Defense, e.g., network operations, CND Services, intelligence, counterintelligence, and law enforcement. CND response can include recommendations or actions by network operations (including information assurance), restoration priorities, law enforcement, military forces, and other US government agencies. (DOD Directive 8530.1)

Computer Network Defense (CND) Operational Hierarchy. The way the Department of Defense is organized to conduct CND. The Department is organized into three tiers to conduct CND. Tier One provides DOD-wide CND operational direction or support to all DOD Components. Tier Two provides DOD Component-wide operational direction or support and responds to direction from Tier One. Tier Three provides local operational direction or support and responds to direction from a designated Tier Two entity. Tier One entities include the US Strategic Command and supporting entities such as the CND Service Certification Authorities, the Defense Criminal Investigative Organization Law Enforcement and Counterintelligence Center, and the National Security Incident Response Center. Tier Two includes CND Service providers designated by heads of components to coordinate component-wide CND. Tier Three includes all entities responding to direction from DOD Component Tier Two CND Service (e.g., local control centers that manage and control information systems, networks and services, either deployed or fixed at DOD Installations). (CJCSI 6510.01)

concept of operations. Document detailing the method, act, process, or effect of using an information system. (CNSS Instruction No. 4009)

confidentiality. Assurance that information is not disclosed to unauthorized persons, processes, or devices. (CNSS Instruction No. 4009)

configuration management. Management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life-cycle of the information technology. (DODI 5200.40]

connection approval. Formal authorization to interconnect information systems. (DODD 8500.1)

contingency plan. Plan maintained for emergency response, backup operations, and post-disaster recovery for an information system, to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency situation. (CNSS Instruction No. 4009)

continuity of operations plan. Plan for continuing an organization's (usually a headquarters element) essential functions at an alternate site and performing those functions for the duration of an event with little or no loss of continuity before returning to normal operations. (CNSS Instruction No. 4009)

controlled interface. A mechanism that facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system) (DCID 6/3).

counterintelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations or foreign persons, or international terrorist activities. (JP 1-02)

controlled access protection. The command and control level of protection described in the Trusted Computer System Evaluation Criteria (Orange Book). Its major characteristics are: individual accountability, audit, access control, and object reuse. These characteristics will be embodied in the National Security Agency-produced controlled access protection profile (and its related follow-on profiles). (CNSS Instruction No. 4009)

controlled unclassified information. Unclassified information to which access or distribution limitations have been applied in accordance with national laws, policies, and regulations of the originating country. It includes US information that is determined to be exempt from public disclosure in accordance with DOD Directives 5230.25 (reference bb) and 5400.7 (reference hh) or that is subject to export controls in accordance with the international traffic in arms regulations (reference ff) or the export administration regulations (reference gg).

criticality. A measure of how important the correct and uninterrupted functioning of the system is to national security, human life, safety, or the mission of the using organization; the degree to which the system performs critical processing. (CJCSM 6510.01)

cryptographic information. All information significantly descriptive of cryptographic techniques and processes or of cryptographic systems and equipment, or their functions and capabilities, and all cryptomaterial. (JP 1-02)

data. Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or automatic means. Any representations such as characters or analog quantities to which meaning is or might be assigned. (JP 1-02)

data integrity. Condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed. (CNSS Instruction No. 4009)

defense critical infrastructures. Those physical and cyber-based systems and assets essential to mobilize, deploy, and sustain military operations and transition to post-conflict military operations, and whose loss or degradation jeopardize the ability of the Department of Defense to execute the National Military Strategy. (CJCSM 6510.01)

defense-in-depth. The DOD approach for establishing an adequate information assurance (IA) posture in a shared risk environment that allows for shared mitigation through: the integration of people, technology and operations; the layering of IA solutions within and among information technology assets; and the selection of IA solutions based on their relative level of robustness. (DODD 8500.1)

defense information infrastructure (DII). The shared or interconnected system of computers, communications, data applications, security, people, training, and other support structures serving DOD local, national, and worldwide information needs. The DII connects DOD mission support, command and control, and intelligence computers through voice, telecommunications, imagery, video, and multimedia services. It provides information processing and services to subscribers over the Defense Information Systems Network and includes command and control, tactical, intelligence, and commercial communications systems used to transmit DOD information. (JP 1-02)

Defense Information Systems Network. The DOD consolidated worldwide enterprise level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations. (DODD 8500.1)

denial of service (attack). Type of incident resulting from any action or series of actions that prevents any part of an information system from functioning. (CNSS Instruction No. 4009)

DOD Information Technology Security Certification and Accreditation Process. The standard DOD process for identifying information security requirements, providing security solutions, and managing information system security activities. (DOD 5200.40)

designated accrediting authority. Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with designated approving authority and delegated accrediting authority. (CNSS Instruction No. 4009)

designated disclosure authority (DDA). An official, designated by the head of a DOD component or by that DOD component's principal disclosure authority, who has been delegated disclosure authority in accordance with DOD Directive 5230.11, to control disclosures by subordinate commands or staff elements of classified military information to foreign governments and their nationals and to international organizations. (DOD Directive 5230.20)

digital signature. Cryptographic process used to assure message originator authenticity, integrity, and non-repudiation. (CNSS Instruction No. 4009)

Discretionary Access Control (DAC). A means of restricting access to objects (e.g., files, data entities) based on the identity and need-to-know of subjects (e.g., users, processes) and/or groups to which the object belongs. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control). (DODI 8500.2)

electronic messaging services. Services providing interpersonal messaging capability; meeting specific functional, management, and technical requirements; and yielding a business-quality electronic mail service suitable for the conduct of official government business. (CNSS Instruction No. 4009)

electronic protection. That division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. (JP 1-02)

electronic surveillance. The acquisition of the contents of a nonpublic communication by electronic means without the consent of a person who is a party to the communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter. (NTISSD No. 600)

emissions security. Protection resulting from measures taken to deny unauthorized individuals information derived from intercept and analysis of compromising emanations from crypto-equipment or an information system. (CNSS Instruction No. 4009)

enclave. Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. (CNSS Instruction No. 4009) Enclaves always assume the highest mission assurance category and security classification of the automated information systems applications or outsourced information technology-based processes they support and derive their security needs from those systems. They provide standard information assurance capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications such as office automation and electronic mail. Enclaves are analogous to general support systems as defined in OMB A-130 (reference qq). Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers. (DODI 8500.2)

enclave boundary. The point at which an enclave's internal network service layer connects to an external network's service layer. (DODI 8500.2)

encryption. To convert plain text into unintelligible forms by means of a cryptosystem. (Note: The term "encrypt" covers the meanings of "encipher" and "encode.") (JP 1-02)

evaluated products list (EPL). Equipment, hardware, software, and/or firmware evaluated by the National Communications Security Center in accordance with DOD trusted computer system evaluation criteria and found to be technically compliant at a particular level of trust. The EPL is included in the National Security Agency Information Systems Security Products and Services Catalogue. (CNSS Instruction No. 4009)

event. Occurrence, not yet assessed, that may affect the performance of an information system. (CNSS Instruction No. 4009)

External Certificate Authority (ECA). An external (outside DOD) agent that is trusted and authorized to create, sign, and issue certificates to approved vendors and contractors for the purpose of enabling secure interoperability with DOD entities. Operating requirements for ECAs must be approved by the DOD Chief Information Officer, in coordination with the DOD Comptroller and the OSD General Counsel. (CJCSM 6510.01)

firewall. System designed to defend against unauthorized access to or from a private network. (CNSS Instruction No. 4009)

foreign exchange personnel. Military or civilian officials of a foreign defense establishment (i.e., a DOD equivalent) who are assigned to a DOD component in accordance with the terms of an exchange agreement and who perform duties, prescribed by a position description, for the DOD component. (DODD 5230.20)

foreign liaison officer (FLO). A foreign government military member or civilian employee who is authorized by his or her government and is certified by a DOD component to act as an official representative of that government in its dealings with a DOD Component in connection with programs, projects, or agreements of interest to the governments. There are three types of FLOs:

a. Security Assistance. A foreign government representative who is assigned to a DOD Component or contractor facility pursuant to a requirement that is described in a Foreign Military Sales Letter of Offer and Acceptance.

b. Operational. A foreign government representative who is assigned to a DOD component pursuant to a documented requirement to coordinate operational matters, such as combined planning or training and education.

c. National Representative. A foreign government representative who is assigned to his or her national embassy or legation in Washington, D.C., (e.g., an attaché) to conduct liaison activities with the Department of Defense and the DOD components. (DODD 5230.20)

foreign national. A person who is not a citizen or national of the United States. (DODD 5230.20)

formal access approval. Process for authorizing access to classified or sensitive information with specified access requirements, such as sensitive compartmented information or privacy data, based on the specified access requirements and a determination of the individual's security eligibility and need-to-know. (CNSS Instruction No. 4009)

freeware. Also known as free software. Software that is free from licensing fees and has no restrictions on use; it can be freely copied, redistributed, or modified. [DOD CIO G&P Guidance Memorandum reference x) Note: Users must comply with regulatory procedures concerning the introduction of freeware onto DOD information systems. (CJCSM 6510.01)

functional domain. An identifiable DOD functional mission area. For purposes of this policy memorandum, the functional domains are: command and control, space, information operations, weapon systems, communications and broadcast, navigation, modeling and simulation, logistics, transportation, health affairs, personnel, financial services, public works, research and development, and intelligence, surveillance, and reconnaissance. (CJCSM 6510.01)

Global Information Grid (GIG). Globally interconnected, end-to-end of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services and other associated services necessary to achieve information superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all DOD, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical, and business), in war and peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalitions, allied and non-DOD users and systems. Non-GIG information technology (IT) is stand-alone, self-contained, or embedded IT that is not or will not be connected to the enterprise network. The GIG includes any system, equipment, software, or service that meets one or more of the following criteria:

a. Transmits information to, receive information from, routes information among, or interchanges information among other equipment, software, and services.

b. Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services.

c. Processes data or information for use by other equipment, software, and services. (DODI 8500.2)

guard. Mechanism limiting the exchange of information between systems. (CNSS Instruction No. 4009)

Intelligence Community member. Agencies, departments, or organizations that produce, process, handle, transfer, and receive intelligence information. (CJCSM 6510.01)

incident. Assessed occurrence having actual or potentially adverse effects on an information system. (CNSS Instruction No.4009).

incident handling. The detection, analysis, and response to any event or incident for the purpose of mitigating any adverse operational or technical impact. (CJCSM 6510.01)

incident set. Any compilation of incidents and/or intrusion sets with similar characteristics. (CJCSM 6510.01)

identification. Process an information system uses to recognize an entity. (CNSS Instruction No. 4009)

information. Any communication or representation of knowledge such as facts, data, or opinion in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. (DODI

8500.2)

information assurance. Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. Note: This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (DODI 8500.2)

information assurance control. An objective information assurance condition of integrity, availability, or confidentiality achieved through the application of specific safeguards or through the regulation of specific activities that is expressed in a specified format, i.e., a control number, a control name, control text, and a control class. (DODI 8500.2)

information system security engineering. An engineering process that captures and refines information protection requirements and ensures their integration into information technology acquisition processes through purposeful security design or configuration. (DODI 8500.2)

Information Assurance Vulnerability Alert (IAVA). The comprehensive distribution process for notifying combatant commands, Services, and agencies (C/S/As) about vulnerability alerts and countermeasures information. The IAVA process requires C/S/A receipt acknowledgment and provides specific time parameters for implementing appropriate countermeasures depending on the criticality of the vulnerability. (CJCSM 6510.01)

information environment. The aggregate of individuals, organizations, or systems that collect, process, or disseminate information, including the information itself. (JP 1-02)

information operations condition (INFOCON). INFOCON is a defense posture and response system for DOD information systems and networks. (CJCSI 6510.01) Note: INFOCON levels are: INFOCON 5 – Normal readiness procedures. INFOCON 4 – Increased military vigilance procedures . INFOCON 3 – Enhanced readiness procedures. INFOCON 2 – Greater readiness procedures. INFOCON 1 – Maximum readiness procedures. (SD 527-1)

information producer. A person, group, or organization that creates, updates, distributes, and retires information based on their authorized and/or assigned missions and functions. (DOD CIO G&P guidance memorandum) information system. Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. (CNSS Instruction No. 4009)

information assurance manager. The individual responsible for the information assurance program of a DOD information system or organization. While the term "information assurance manager" is favored within the Department of Defense, it may be used interchangeably with the information assurance title "information systems security manager." (DODI 8500.2)

information assurance officer. An individual responsible to the information assurance (IA) manager for ensuring the appropriate operational IA posture is maintained for a DOD information system or organization. While the term "information assurance officer" is favored within the Department of Defense, it may be used interchangeably with other IA titles, e.g., "information systems security officer," "information systems security custodian," "network security officer," or "terminal area security officer." (DODI 8500.2)

information superiority. The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (JP 1-02)

integrity. Quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that in a formal security mode integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information. (CNSS Instruction No. 4009)

Intelligence Community information. Sensitive compartmented information and any other information that is classified pursuant to section 1.5(c) of Executive Order 12958 and also bears special intelligence handling markings found in the "Authorized Classification and Control Markings Registry" maintained by the Community Management Staff. (CJCSM 6510.01)

interconnected. An interconnected information system is composed of separately accredited information systems (i.e., Enclaves). Each self-contained information system maintains its own intra-system services and controls, protects its own resources, and retains its individual accreditation. Each participating information system has its own information assurance office. (CJCSM 6510.01) intrusion. Unauthorized act of bypassing the security mechanisms of a system. (CNSS Instruction No. 4009)

joint vulnerability assessment process. Process including evaluation and development of automated tools for measuring system risks that are operated by the National Security Agency and Defense Information Systems Agency against SECRET and Below Interoperability connection implementations to ensure Global Information Grid integrity. (CJCSM 6510.01)

layered defense. A combination of security services, software and hardware, infrastructures, and processes that are implemented to achieve a required level of protection. These mechanisms are additive in nature, with the minimum protection being provided by the network and infrastructure layers. (CJCSM 6510.01)

level of concern. A rating assigned to an information system that indicates the extent to which protective measures, techniques, and procedures must be applied. The Department of Defense has three levels of concern: a. High — Information systems that require the most stringent protection measures and rigorous countermeasures. b. Medium — Information systems that require layering of additional safeguards above the DOD minimum standard (Basic). c. Basic — Information systems that require implementation of the DOD minimum standard. (CJCSM 6510.01)

level of robustness. The characterization of the strength of a security function, mechanism, service, or solution, and the assurance (or confidence) that it is implemented and functioning correctly to support the level of concern assigned to a particular information system. The Department of Defense has three levels of robustness: a. High — Security services and mechanisms that provide the most stringent available protection and rigorous security countermeasures. b. Medium — Security services and mechanisms that provide for layering of additional safeguards above the DOD minimum (LB) (Basic). c. Basic — Security services and mechanisms that equate to good commercial practices. (CJCSM 6510.01)

local area network (LAN). A data communications system that (a) lies within a limited spatial area, (b) has a specific user group, (c) has a specific topology, and (d) is not a public switched telecommunications network, but may be connected to one. Note 1: LANs are usually restricted to relatively small areas, such as rooms, buildings, ships, and aircraft. Note 2: An interconnection of LANs within a limited geographical area, such as a military base, is commonly referred to as a campus area network. An interconnection of LANs over a citywide geographical area is commonly called a metropolitan area network. An interconnection of LANs over large geographical areas, such as nationwide, is commonly called a wide area network (WAN). Note 3: LANs are not subject to public telecommunications regulations. (Federal Standard 1037C)

malicious code. Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. (CNSS Instruction No. 4009)

malicious logic. Hardware, software, or firmware capable of performing an unauthorized function on an information system. (CNSS Instruction No. 4009)

memorandum of agreement (MOA). A written agreement among the designated approving authorities (DAAs) responsible for the information processed and maintained by an information system (or collection of systems). The MOA stipulates all of the terms and conditions of the security arrangements that will govern the operation of the information system(s). The MOA shall include at least: (1) a general description of the information to be offered by each participating DAA; and (2) a discussion of all of the security details pertinent to the exchange of information between the DAAs. A lead DAA and description of the types of information serves provided will be in the MOA to cover interconnected network of information systems under the purview of different DAAs. If no lead DAA is named, then both parties share responsibility. (CJCSM 6510.01)

mission assurance category (MAC). Applicable to DOD information systems, the MAC reflects the importance of information relative to the achievement of DOD goals and objectives, particularly the warfighters' combat mission. MACs are primarily used to determine the requirements for availability and integrity. The Department of Defense has three defined mission assurance categories:

a. MAC I. Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.

b. MAC II. Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure assurance.

c. MAC III. Systems handling information that is necessary for the conduct of day-to-day business but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques, or procedures generally commensurate with commercial best practices. (DODI 8500.2)

mobile code. Software modules obtained from remote systems, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient. (DODI 8500.2)

National Information Assurance Partnership. Joint initiative between the National Security Agency and the National Institute of Standards and Technology for security testing needs of both information technology (IT) consumers and producers and promoting the development of technically sound security requirements for IT products and systems and appropriate measures for evaluating those products and systems. (DODI 8500.2)

national information infrastructure (NII). The NII is a system of high-speed telecommunications networks, databases, and advanced computer systems that will make electronic information widely available and accessible. Although the NII is being designed, built, owned, operated, and used by the private sector, the government makes significant use of the NII. The NII includes the Internet, the public switched network, and cable, wireless, and satellite communications. It includes public and private networks. (CJCSM 6510.01)

national security systems. Any telecommunications or information system operated by the US government, the function, operation, or use of which: 1. involves intelligence activities; 2. involves cryptologic activities related to national security; 3. involves command and control of military forces; 4. involves equipment that is an integral part of a weapon or weapon system; or 5. is critical to the direct fulfillment of military or intelligence missions and does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). (CNSS Instruction No. 4009)

network. Information system implemented with a collection of interconnected nodes. (CNSS Instruction No. 4009)

network architecture. 1. The design principles, physical configuration, functional organization, operational procedures, and data formats used as the bases for the design, construction, modification, and operation of a communications network. 2. The structure of an existing communications network, including the physical configuration, facilities, operational structure, operational procedures, and the data formats in use. (Federal Standard 1037C)

nonpublic communication. A communication in which the parties thereto have a reasonable expectation of privacy. (NTISSD No. 600)

non-repudiation. Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender’s identity, so neither can later deny having processed the data. (CNSS Instruction No. 4009)

Non-classified Internet Protocol Routing Network (NIPRNET). Unclassified but sensitive Internet Protocol Network, one of two types of Internet Protocol routers owned by the Defense Information System Network. Note: The NIPRNET contains sensitive information and controlled information that must be protected. See definitions of controlled unclassified information and sensitive information. (DOD Chief Information Officer Annual Information Assurance Report Fiscal Year 2000)

operating system. An integrated collection of routines that service the sequencing and processing of programs by a computer. Note: An operating system may provide many services, such as resource allocation, scheduling, input/output control, and data management. Although operating systems are predominantly software, partial or complete hardware implementations may be made in the form of firmware. (Federal Standard 1037C)

operational threat environment. A generalized overview of the operational, physical, and technological environment in which the system will have to function during its lifetime. Developments and trends that can be expected to affect mission capability during the system’s life span should be included. Areas to be covered should include all generations of threat as outlined by a US command.

a. Threats, first generation: Common hacker tools and techniques used in a non-sophisticated manner. Lone or possibly small groups of amateurs without large resources.

b Threats, second generation: Non-state-sponsored espionage or data theft. Common tools used in a sophisticated manner. Individuals or small groups supported by resources of a business, criminal syndicate or other trans-national group, including terrorists.

c. Threats, third generation: State-sponsored espionage. More sophisticated threat (than first and second) supported by institutional processes and significant resources. (CJCSI 6510.01)

operations security. A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. Identify those actions that can be observed by adversary intelligence systems. b. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries. c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. (JP 1-02)

password. Protected and/or private strings of letters, numbers, and special characters used to authenticate an identity or to authorize access to data. (CNSS Instruction No. 4009)

physical security. That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. (JP 1-02)

protection philosophy. Informal description of the overall design of an information system delineating each of the protection mechanisms employed. Combination of formal and informal techniques, appropriate to the evaluation class, used to show the mechanisms are adequate to enforce the security policy. (CNSS Instruction No. 4009)

protection level. An indication of the implicit level of trust that is placed in a system's technical capabilities. A protection level is based on the classification and sensitivity of information processed on the system relative to the clearance(s), formal access approval(s), and need-to-know of all direct and indirect users that receive information from the information system without manual intervention and reliable human review.  (DCID 6/3)

protected distribution systems (PDS).  Wire line or fiber optic distribution system used to transmit unencrypted classified national security information through an area of lesser classification or control.  (CNSS Instruction No. 4009)

public key infrastructure.  Framework established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies, including the use of software.  (CNSS Instruction No. 4009)

purging.  Rendering stored information unrecoverable.  (CNSS Instruction No. 4009)

push only technology.  The means by which data is presented to a user without a specific action initiated by that user.  In client-server terminology, the server initiates, or "pushes," the data to the client, usually in accordance with a pre-established user profile.  This interest profile typically contains information categories of interests (e.g., weather forecasts, stock quotes).  (CJCSM 6510.01)

push/pull technology.  A combination of technologies for information dissemination and retrieval.  Traditionally, data is retrieved by a user request, such as by a Web user.  In this case, the user "pulls" information.  Alternatively, an information server may "push" information to the client without client intervention, usually by applying a predefined profile that filters information.  (CJCSM 6510.01)

real-time reaction.  Immediate response to a penetration attempt that is detected and diagnosed in time to prevent access.  (CNSS Instruction No. 4009)

red team.  Independent and focused threat-based effort by an interdisciplinary, simulated adversary to expose and exploit vulnerabilities as a means to improve the security posture of information systems.  (CNSS Instruction No. 4009)

reliable human review.  Any manual, automated, or combined process or procedure for opening and reviewing digital objects (e.g., files, images) to ensure that the digital object can be transferred across a controlled interface.  (CJCSM 6510.01) remote access. Enclave-level access for authorized users that are external to the enclave that is established through a controlled access point at the enclave boundary. (DODI 8500.2)

remote diagnostics/maintenance. The operational procedure that involves connection of a system to an external (i.e., outside of the facility securing the system) remote service for analysis or maintenance. (CJCSM 6510.01)

risk analysis. Probability and severity of loss linked to hazards. (JP 1-02)

risk assessment. Process of analyzing threats to and vulnerabilities of an information system and the potential impact resulting from the loss of information or capabilities of a system. The analysis is used as a basis for identifying appropriate and cost-effective countermeasures. (CNSS Instruction No. 4009)

risk index. Difference between the minimum clearance or authorization of information system users and the maximum sensitivity (e.g., classification and categories) of data processed by the system. (CNSS Instruction No. 4009)

risk management. Process of identifying and applying countermeasures commensurate with the value of the assets protected based on a risk assessment. (CNSS Instruction No. 4009)

router. In data communications, a functional unit used to interconnect two or more networks. Note 1: Routers operate at the network layer (layer 3) of the ISO Open Systems Interconnection—Reference Model. Note 2: The router reads the network layer address of all packets transmitted by a network and forwards only those addressed to another network. (Federal Standard 1037C)

SECRET and Below Interoperability. An Assistant to the Secretary of Defense (Command, Control, Communications, and Intelligence)-directed, Joint Chiefs of Staff-sponsored, National Security Agency/Defense Information Systems Agency-executed initiative to enhance SECRET and Below Interoperability, measure community risk, and protect the Global Information Grid information systems infrastructure. (CJCSM 6510.01)

SECRET Internet Protocol Router Network. Worldwide SECRET level packet switch network that uses high-speed Internet protocol routers and high-capacity Defense Information Systems Network circuitry. (JP 1-02)

security domain. Refers to a discrete information system identified by its authorized classification level and releasability and administrative controls. It does not refer to information systems interconnection of compartments at the same classification level. Manual transfer processes or controlled interfaces are required to transfer information between security domains that operate under different security policies. (CJCSM 6510.01)

security incident. An attempt to exploit a national security system such that the actual or potential adverse effects may involve fraud, waste, or abuse; compromise of information; loss or damage of property or information; or denial of service. Security incidents include penetration of computer systems, exploitation of technical and administrative vulnerabilities, and introduction of computer viruses or other forms of malicious code. (A security incident may also involve a violation of law. If a violation of law is evident or suspected, the incident must also be reported to both security and law enforcement organizations for appropriate action.) (NSTISSD 503)

security incident response. Actions conducted to resolve information systems security incidents and protect national security systems. (NSTISSD 503)

security label. A piece of information that represents the hierarchical classification (CONFIDENTIAL, SECRET, or TOP SECRET) and non-hierarchical compartments (e.g., specific sensitive compartmented information or special access program controls) of a subject or object and that thus describes the sensitivity of the data in the subject or object. Security labels are used as the basis for mandatory access control. (CJCSM 6510.01)

security markings. Indicators applied to a document, storage media, or hardware component to designate categorization and handling restrictions applicable to the information in the document. For intelligence information, these could include compartment and sub-compartment indicators and handling restrictions. For DOE information, these could include indicators of information type (such as Restricted Data) and Sigma categories. (DCID 6/3)

security penetration testing. System testing designed to evaluate the relative vulnerability of the system to hostile attacks. Penetration testers often try to obtain unauthorized privileges (especially attempts to obtain "root" or "superuser" privileges) by exploiting flaws in system design or implementation. (CJCSM 6510.01)

security safeguards. Protective measures and controls prescribed to meet the security requirements specified for an information system.

Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. See accreditation. (CNSS Instruction No. 4009)

security support structure. Those components of a system (hardware, firmware, software, data, interfaces, storage media, and communications media) that are essential to the enforcement of the system's security policies. (CJCSM 6510.01)

Security Technical Implementation Guide. A guide for information security. A compendium of security regulations and best practices from many sources that apply to an operating system or a part of the GIG infrastructure. (CJCSM 6510.01)

sensitive compartmented information. Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence. (DODI 8500.2
)

sensitive information. Information, the loss, misuse, or unauthorized access to or modification of, could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under Section 552a of title 5, United States Code, "The Privacy Act," but which has not been specifically authorized under criteria established by executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy. (Section 278g-3 of title 15, United States Code, "The Computer Security Act of 1987.") Examples of sensitive information include, but are not limited to, information in DOD payroll, finance, logistics, and personnel management systems. Sensitive information subcategories include, but are not limited to, the following:

a. For Official Use Only (FOUO). In accordance with DOD 5400.7-R, DOD information exempted from mandatory public disclosure under the Freedom of Information Act (FOIA).

b. Privacy Data. Any record that is contained in a system of records as defined in the Privacy Act of 1974 (5 USC 552a) and information the disclosure of which would constitute an unwarranted invasion of personal privacy.

c. DOD Unclassified Controlled Nuclear Information (DOD UCNI). Unclassified information on security measures (including security plans, procedures, and equipment) for the physical protection of DOD Special Nuclear Material (SNM), equipment, or facilities in accordance with DOD Directive 5210.83. Information is designated DOD UCNI only when it is determined that its unauthorized disclosure could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by increasing significantly the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of DOD SNM, equipment, or facilities.

d. Unclassified Technical Data. Data that is not classified but is subject to export control and is withheld from public disclosure according to DOD Directive 5230.25.

e. Proprietary Information. Information that is provided by a source or sources under the condition that it not be released to other sources.

f. Foreign Government Information. Information that originated from a foreign government and that is not classified CONFIDENTIAL or higher but must be protected in accordance with DOD 5200.1-R.

g. Department of State Sensitive But Unclassified (DoS SBU). Information that originated from the Department of State (DOS) that has been determined to be SBU under appropriate DOS information security polices.

h. Drug Enforcement Administration (DEA) Sensitive Information. Information that is originated by the Drug Enforcement Administration and requires protection against unauthorized disclosure to protect sources and methods of investigative activity, evidence, and the integrity of pretrial investigative reports. (DODI 8500.2)

special enclave network. DOD information systems and/or computer networks with special security requirements (e.g. special access program, special access requirements, and designated as special enclave by the Assistant Secretary of Defense (Command, Control, Communications and Intelligence). (DOD Instruction O-8530.2)

strong authentication. A form of authentication whereby it is very difficult or impossible for a hostile user to successfully intercept and employ a transmitted authenticator (i.e., highly resistant to replay attack). (CJCSM 6510.01)

strong binding. A mechanism that provides an explicit link (e.g., cryptographic association) between an end entity (e.g., individual user, author, reliable human reviewer) and data. The binding provides traceability (proof of origin, attribution, non-repudiation capability) of the data to the end entity. The binding (integrity seal) is also used to detect unauthorized modification of or tampering with the data. An example of a strong binding is a cryptographic digital signature. (CJCSM 6510.01)

susceptibility. Technical characteristics describing inherent limitations of a system that have potential for exploitation. (CJCSM 6510.01)

survivability. The ability of a computer and/or communications system-based application to satisfy and to continue to satisfy certain critical requirements (e.g., specific requirements for security, reliability, real-time responsiveness, and correctness) in the face of adverse conditions. (CJCSM 6510.01)

system administrator. Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established information assurance policy and procedures. (CNSS Instruction No. 4009)

system high mode. Information system (IS) security mode of operation wherein each user, with direct or indirect access to the IS, its peripherals, remote terminals, or remote hosts, has all of the following: a. valid security clearance for all information within an IS; b. formal access approval and signed nondisclosure agreements for all the information stored and/or processed (including all compartments, subcompartments, and/or special access programs); and c. valid need-to-know for some of the information contained within the IS. (CNSS Instruction No. 4009)

target. A computer or network logical entity (account, process, or data) or physical entity (component, computer, network or internet network). (CJCSI 6510.01)

technical vulnerability. A hardware, firmware, or software weakness or design deficiency that leaves an information system open to potential exploitation, either externally or internally, thereby resulting in risk of compromise of information, alteration of information, or denial of service. (NSTISSD 503)

technique. A means of exploiting a computer or network vulnerability. (CJCSI 6510.01)

telecommunications. Preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means. (CNSS Instruction No. 4009)

TEMPEST. An unclassified term referring to technical investigations for compromising emanations from electrically operated information-processing equipment; these investigations are conducted in support of emanations and emissions security. (JP 1-02)

threat. Any circumstance or event with the potential to adversely impact an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. (CNSS Instruction No. 4009)

transmission security. Component of communications security resulting from the application of measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. (CNSS Instruction No. 4009)

unauthorized result. An unauthorized consequence of an event. (CJCSI 6510.01)

US classified cryptographic information. 1. TOP SECRET and SECRET, CRYPTO designated, key, and authenticators. 2. All cryptographic media that embody, describe, or implement classified cryptographic logic; this includes full maintenance manuals, cryptographic descriptions, drawings of cryptographic logic, specifications describing a cryptographic logic, cryptographic computer software, or any other media that may be specifically identified by the National Security Telecommunications and Information System Security Committee (NSTISSC). (CJCSI 6510.01)

unclassified information. Information that has not been determined pursuant to Executive Order 12958 or any predecessor order to require protection against unauthorized disclosure and that is not designated as classified. (CNSS Instruction No. 4009)

US nongovernmental source. An individual US citizen or a US corporation, association, or other organization substantially composed of US citizens, that is not directly a part of the US government (for example, a self-employed individual, consulting firm, licensee, or contractor, excluding Active or Reserve military personnel, civil service employees, and other individuals employed directly by the government); specifically excluded are corporations or associations under foreign ownership, control, and influence. (CJCSI 6510.01)

user. Individual or process authorized to access an information system. (CNSS Instruction No. 4009) virtual private network. Protected information system link utilizing tunneling, security controls (see information assurance), and end-point address translation giving the user the impression a dedicated line exists between nodes. (CNSS Instruction No. 4009)

vulnerability. 1. The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. 2. The characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment. 3. In information operations, a weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system. (JP 1-02)

vulnerability analysis. Examination of information to identify the elements comprising a vulnerability. (CNSS Instruction No. 4009)

vulnerability assessment. Formal description and evaluation of vulnerabilities of an information system. (CNSS Instruction No. 4009)